RackSwitch™ G8000
Command Reference

Version 6.0

Part Number: BMD00127, September 2009

BLADE NETWORK TECHNOLOGIES

2350 Mission College Blvd.
Suite 600
Santa Clara, CA 95054
www.bladenetwork.net

Contents

Preface

The RackSwitch G8000 *Command Reference* describes how to configure and use the BLADE OS software with your RackSwitch G8000.

For documentation on installing the switches physically, see the *Installation Guide* for your G8000. For details about configuration and operation of your G8000, see the RackSwitch G8000 *Application Guide*.

Who Should Use This Book

This *Command Reference* is intended for network installers and system administrators engaged in configuring and maintaining a network. The administrator should be familiar with Ethernet concepts, IP addressing, the IEEE 802.1D Spanning Tree Protocol, and SNMP configuration parameters.

How This Book Is Organized

Chapter 1 "The Command Line Interface," describes how to connect to the switch and access the information and configuration menus.

Chapter 2 "First-Time Configuration," describes initial switch configuration and how to change the system passwords.

Chapter 3 "Menu Basics," provides an overview of the menu system, including a menu map, global commands, and menu shortcuts.

Chapter 4 "The Information Menu," shows how to view switch configuration parameters.

Chapter 5 "The Statistics Menu," shows how to view switch performance statistics.

Chapter 6 "The Configuration Menu," shows how to configure switch system parameters, ports, VLANs, Spanning Tree Protocol, SNMP, Port Mirroring, IP Routing, Port Trunking, and more.

Chapter 7 "The Operations Menu," shows how to use commands which affect switch performance immediately, but do not alter permanent switch configurations (such as temporarily disabling ports). The menu describes how to activate or deactivate optional software features.

Chapter 8 "The Boot Options Menu," describes the use of the primary and alternate switch images, how to load a new software image, and how to reset the software to factory defaults.

Chapter 9 "The Maintenance Menu," shows how to generate and access a dump of critical switch state information, how to clear it, and how to clear part or all of the forwarding database.

"Index" includes pointers to the description of the key words used throughout the book.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	This type is used for names of commands, files, and directories used within the text.	View the `readme.txt` file.
	It also depicts on-screen computer output and prompts.	`Main#`
`AaBbCc123`	This bold type appears in command examples. It shows text that must be typed in exactly as shown.	`Main#` **`sys`**
<AaBbCc123>	This italicized type appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.	To establish a Telnet session, enter: `host#` **`telnet`** *<IP address>*
	This also shows book titles, special terms, or words to be emphasized.	Read your *User's Guide* thoroughly.
[ ]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	`host#` **`ls`** [**`-a`**]

How to Get Help

If you need help, service, or technical assistance, call Blade Network Technologies Technical Support:

US toll free calls: 1-800-414-5268

International calls: 1-408-834-7871

You also can visit our web site at the following address:

http://www.bladenetwork.net

Click the **Support** tab.

The warranty card received with your product provides details for contacting a customer support representative. If you are unable to locate this information, please contact your reseller. Before you call, prepare the following information:

- Serial number of the switch unit
- Software release version number
- Brief description of the problem and the steps you have already taken
- Technical support dump information (`# show tech-support`)

CHAPTER 1

The Command Line Interface

Your RackSwitch G8000 is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

The extensive BLADE OS switching software included in your switch provides a variety of options for accessing and configuring the switch:

- A built-in, text-based command line interface and menu system for access via a Telnet session or serial-port connection
- SNMP support for access through network management software such as IBM Director or HP OpenView
- BLADE OS Browser-Based Interface (BBI)

The command line interface is the most direct method for collecting switch information and performing switch configuration. Using a basic terminal, you are presented with a hierarchy of menus that enable you to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the Command Line Interface (CLI) for the switch.

Connecting to the Switch

You can access the command line interface in any one of the following ways:

- Using a Telnet connection over the network
- Using a SSH connection to securely log into another computer over a network
- Using a serial connection using the serial port on the G8000

Connecting to the Switch via Telnet

Once you have configured the G8000 with an IP address and gateway, you can access the switch from any workstation connected to the management network.

To establish a Telnet connection with the switch, run the Telnet program on your workstation and issue the Telnet command, followed by the switch IP address:

```
telnet <switch IP address>
```

Establishing an SSH Connection

Although a remote network administrator can manage the configuration of the G8000 via Telnet, this method does not provide a secure connection. The SSH (Secure Shell) protocol enables you to securely log into another computer over a network to execute commands remotely. As a secure alternative to using Telnet to manage switch configuration, SSH ensures that all data sent over the network is encrypted and secure.

The switch can handle only one session of key/cipher generation at a time. Thus, an SSH/SCP client will not be able to login if the switch is doing key generation at that time or if another client has just logged in before this client. Similarly, the system will fail to do the key generation if a SSH/SCP client is logging in at that time.

The supported SSH encryption and authentication methods are listed below.

- Server Host Authentication: Client RSA-authenticates the switch in the beginning of every connection.
- Key Exchange: RSA
- Encryption: 3DES-CBC, DES
- User Authentication: Local password authentication, Radius

The following SSH clients have been tested:

- SSH 1.2.23 and SSH 1.2.27 for Linux (freeware)
- SecureCRT 3.0.2 and SecureCRT 3.0.3 (Van Dyke Technologies, Inc.)
- F-Secure SSH 1.1 for Windows (Data Fellows)

NOTE – The BLADE OS implementation of SSH is based on SSH version 1 and SSH version 2.

Running SSH

Once the IP parameters are configured and the SSH service is turned on the G8000, you can access the command line interface using an SSH connection. The default setting for SSH access is disabled.

To establish an SSH connection with the switch, run the SSH program on your workstation by issuing the SSH command, followed by the switch IP address:

```
>> # ssh <switch IP address>
```

If SecurID authentication is required, use the following command:

```
>> # ssh -1 ace <switch IP address>
```

You will then be prompted to enter your user name and password.

Accessing the Switch

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the G8000. Levels of access to CLI, Web management functions, and screens increase as needed to perform various switch management tasks. Conceptually, access classes are defined as follows:

- User interaction with the switch is completely passive—nothing can be changed on the G8000. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- Operators can make temporary changes on the G8000. These changes are lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the switch, operators cannot severely impact switch operation.
- Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reboot/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the G8000. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique surnames and passwords. Once you are connected to the switch via local Telnet, remote Telnet, or SSH, you are prompted to enter a password. The default user names/password for each access level are listed in the following table.

NOTE – It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies. For more information, see "Setting Passwords" on page 20.

Table 1-1 User Access Levels

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	`user`
Operator	The Operator manages all functions of the switch. The Operator can reset ports, except the management port.	`oper`
Administrator	The superuser Administrator has complete access to all menus, information, and configuration commands on the G8000, including the ability to change both the user and administrator passwords.	`admin`

NOTE – With the exception of the "admin" user, access to each user level can be disabled by setting the password to an empty value.

Command Line History and Editing

For a description of global commands, shortcuts, and command line editing functions, see "Menu Basics" on page 25."

Idle Timeout

By default, the switch will disconnect your Telnet session after 10 minutes of inactivity. This function is controlled by the idle timeout parameter, which can be set from 1 to 60 minutes. For information on changing this parameter, see "System Configuration" on page 115.

CHAPTER 2

First-Time Configuration

This chapter provides information to help with the initial configuration of your switch.

Setup for Telnet Support

NOTE – This procedure is optional. Perform this procedure only if you are planning on connecting to the switch through a remote Telnet connection.

1. **Telnet is enabled by default. To change the setting, use the following command:**

```
>> # /cfg/sys/access/tnet
```

2. **Apply and save SNMP and /or telnet configuration(s).**

```
>> System# apply
>> System# save
```

Setting Passwords

It is recommended that you change the user and administrator passwords after initial configuration and as regularly as required under your network security policies.

To change the administrator password, you must login using the administrator password.

NOTE – If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

Changing the Default Administrator Password

The administrator has complete access to all menus, information, and configuration commands, including the ability to change both the user and administrator passwords.

The default password for the administrator account is `admin`. To change the default password, follow this procedure:

1. **Connect to the switch and log in using the `admin` password.**
2. **From the Main Menu, use the following command to access the Configuration Menu:**

```
Main# /cfg
```

The Configuration Menu is displayed.

```
[Configuration Menu]
     sys       - System-wide Parameter Menu
     port      - Port Menu
     stack     - Stacking Menu
     qos       - QOS Menu
     acl       - Access Control List Menu
     pmirr     - Port Mirroring Menu
     l2        - Layer 2 Menu
     l3        - Layer 3 Menu
     dump      - Dump current configuration to script file
     ptcfg     - Backup current configuration to FTP/TFTP server
     gtcfg     - Restore current configuration from FTP/TFTP server
     cur       - Display current configuration
```

3. **From the Configuration Menu, use the following command to select the System Menu:**

```
>> Configuration# sys
```

The System Menu is displayed.

```
[System Menu]
     syslog   - Syslog Menu
     sshd     - SSH Server Menu
     radius   - RADIUS Authentication Menu
     tacacs+  - TACACS+ Authentication Menu
     ntp      - NTP Server Menu
     ssnmp    - System SNMP Menu
     access   - System Access Menu
     date     - Set system date
     time     - Set system time
     timezone - Set system timezone
     olddst   - Set system DST for US prior to 2007
     dlight   - Set system daylight savings
     idle     - Set timeout for idle CLI sessions
     notice   - Set login notice
     bannr    - Set login banner
     hprompt  - Enable/disable display hostname (sysName) in CLI prompt
     dhcp     - Enable/disable use of DHCP on Mgmt interface
     rstctrl  - Enable/disable System reset on panic
     cur      - Display current system-wide parameters
```

4. **From the System Menu, use the following command to select the System Access Menu:**

```
>> System# access
```

The System Access Menu is displayed.

```
[System Access Menu]
     mgmt     - Management Network Definition Menu
     user     - User Access Control Menu (passwords)
     https    - HTTPS Web Access Menu
     snmp     - Set SNMP access control
     tnport   - Set Telnet server port number
     tport    - Set the TFTP Port for the system
     wport    - Set HTTP (Web) server port number
     http     - Enable/disable HTTP (Web) access
     tnet     - Enable/disable Telnet access
     tsbbi    - Enable/disable Telnet/SSH configuration from BBI
     userbbi  - Enable/disable user configuration from BBI
     cur      - Display current system access configuration
```

5. **Select the administrator password.**

```
System Access# user/admpw
```

6. **Enter the current administrator password at the prompt:**

```
Changing ADMINISTRATOR password; validation required...
Enter current administrator password:
```

NOTE – If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

7. **Enter the new administrator password at the prompt:**

```
Enter new administrator password:
```

8. **Enter the new administrator password, again, at the prompt:**

```
Re-enter new administrator password:
```

9. **Apply and save your change by entering the following commands:**

```
System# apply
System# save
```

Changing the Default User Password

The user login has limited control of the switch. Through a user account, you can view switch information and statistics, but you can't make configuration changes.

The default password for the user account is `user`. This password can be changed from the user account. The administrator can change all passwords, as shown in the following procedure.

1. **Connect to the switch and log in using the `admin` password.**
2. **From the Main Menu, use the following command to access the Configuration Menu:**

```
Main# cfg
```

3. **From the Configuration Menu, use the following command to select the System Menu:**

```
>> Configuration# sys
```

4. **From the System Menu, use the following command to select the System Access Menu:**

```
>> System# access
```

5. **Select the user password.**

```
System# user/usrpw
```

6. **Enter the current administrator password at the prompt.**

   Only the administrator can change the user password. Entering the administrator password confirms your authority.

```
Changing USER password; validation required...
Enter current administrator password:
```

7. **Enter the new user password at the prompt:**

```
Enter new user password:
```

8. **Enter the new user password, again, at the prompt:**

```
Re-enter new user password:
```

9. **Apply and save your changes:**

```
System# apply
System# save
```

CHAPTER 3

Menu Basics

The G8000's Command Line Interface (CLI) is used for viewing switch information and statistics. In addition, the administrator can use the CLI for performing all levels of switch configuration.

To make the CLI easy to use, the various commands have been logically grouped into a series of menus and sub-menus. Each menu displays a list of commands and/or sub-menus that are available, along with a summary of what each command will do. Below each menu is a prompt where you can enter any command appropriate to the current menu.

This chapter describes the Main Menu commands, and provides a list of commands and shortcuts that are commonly available from all the menus within the CLI.

The Main Menu

The Main Menu appears after a successful connection and login. The following table shows the Main Menu for the administrator login. Some features are not available under the user login.

```
[Main Menu]
     info     - Information Menu
     stats    - Statistics Menu
     cfg      - Configuration Menu
     oper     - Operations Command Menu
     boot     - Boot Options Menu
     maint    - Maintenance Menu
     diff     - Show pending config changes  [global command]
     apply    - Apply pending config changes [global command]
     save     - Save updated config to FLASH [global command]
     revert   - Revert pending or applied changes [global command]
     exit     - Exit  [global command, always available]
```

Menu Summary

- **Information Menu**

  Provides sub-menus for displaying information about the current status of the switch: from basic system settings to VLANs, and more.

- **Statistics Menu**

  Provides sub-menus for displaying switch performance statistics.

- **Configuration Menu**

  This menu is available only from an administrator login. It includes sub-menus for configuring every aspect of the switch. Changes to configuration are not active until explicitly applied. Changes can be saved to non-volatile memory.

- **Operations Command Menu**

  Operations-level commands are used for making immediate and temporary changes to switch configuration. This menu is used for bringing ports temporarily in and out of service, performing port mirroring, and so on.

- **Boot Options Menu**

  This menu is used for upgrading switch software, selecting configuration blocks, and for resetting the switch when necessary.

- **Maintenance Menu**

  This menu is used for debugging purposes, enabling you to generate a dump of the critical state information in the switch, and to clear entries in the forwarding database and the ARP tables.

Global Commands

Some basic commands are recognized throughout the menu hierarchy. These commands are useful for obtaining online help, navigating through menus, and for applying and saving configuration changes.

For help on a specific command, type `help`. You will see the following screen:

```
Global Commands: [can be issued from any menu]
help              up                print             pwd
lines             verbose           exit              quit
diff              apply             save              revert
revert apply
ping              traceroute        telnet            history
pushd             popd              who               chpass_p
chpass_s

The following are used to navigate the menu structure:
    .  Print current menu
   ..  Move up one menu level
    /  Top menu if first, or command separator
    !  Execute command from history
```

Table 3-1 Description of Global Commands

Command	Action
? *command* **or help**	Provides more information about a specific command on the current menu. When used without the *command* parameter, a summary of the global commands is displayed.
. or print	Display the current menu.
.. or up	Go up one level in the menu structure.
/	If placed at the beginning of a command, go to the Main Menu. Otherwise, this is used to separate multiple commands placed on the same line.
lines	Set the number of lines (n) that display on the screen at one time. The default is 24 lines. When used without a value, the current setting is displayed. Set lines to a value of 0 (zero) to disable pagination.
diff	Show any pending configuration changes.
apply	Apply pending configuration changes.
save	Write configuration changes to non-volatile flash memory.

Table 3-1 Description of Global Commands

Command	Action
revert	Remove pending configuration changes between "apply" commands. Use this command to restore configuration parameters set since last `apply`.
revert apply	Remove pending or applied configuration changes between "`save`" commands. Use this command to remove any configuration changes made since last `save`.
exit or quit	Exit from the command line interface and log out.
ping	Use this command to verify station-to-station connectivity across the network. The format is as follows: **ping** *<host name> | <IP address>* [*tries (1-32)> [msec delay*]] Where *IP address* is the hostname or IP address of the device, *tries* (optional) is the number of attempts (1-32), *msec delay* (optional) is the number of milliseconds between attempts. The DNS parameters must be configured if specifying hostnames (see "Domain Name System Configuration" on page 184).
traceroute	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: **traceroute** *<host name>| <IP address>* [*<max-hops (1-32)>* [*msec delay*]] Where *IP address* is the hostname or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-32 devices), and *delay* (optional) is the number of milliseconds for wait for the response. As with `ping`, the DNS parameters must be configured if specifying hostnames.
pwd	Display the command path used to reach the current menu.
verbose *n*	Sets the level of information displayed on the screen: **0** =Quiet: Nothing appears except errors—not even prompts. **1** =Normal: Prompts and requested output are shown, but no menus. **2** =Verbose: Everything is shown. When used without a value, the current setting is displayed.
telnet	This command is used to telnet out of the switch. The format is as follows: **telnet** *<hostname> | <IP address>* [port] Where *IP address* is the hostname or IP address of the device.
history	This command displays the most recent commands.
pushd	Save the current menu path, so you can jump back to it using `popd`.
popd	Go to the menu path and position previously saved by using `pushd`.
who	Displays a list of users that are logged on to the switch.

Table 3-1 Description of Global Commands

Command	Action
chpass_p	Configures the password for the primary TACACS+ server.
chpass_s	Configures the password for the secondary TACACS+ server.

Command Line History and Editing

Using the command line interface, you can retrieve and modify previously entered commands with just a few keystrokes. The following options are available globally at the command line:

Table 3-2 Command Line History and Editing Options

Option	Description
`history`	Display a numbered list of the last 64 previously entered commands.
`!!`	Repeat the last entered command.
`!`*n*	Repeat the n^{th} command shown on the history list.
<Ctrl-p>	(Also the up arrow key.) Recall the *previou*s command from the history list. This can be used multiple times to work backward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-n>	(Also the down arrow key.) Recall the *next* command from the history list. This can be used multiple times to work forward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-a>	Move the cursor to the beginning of command line.
<Ctrl-e>	Move cursor to the *end* of the command line.
<Ctrl-b>	(Also the left arrow key.) Move the cursor *back* one position to the left.
<Ctrl-f>	(Also the right arrow key.) Move the cursor *forward* one position to the right.
<Backspace>	(Also the Delete key.) Erase one character to the left of the cursor position.
<Ctrl-d>	*Delete* one character at the cursor position.
<Ctrl-k>	*Kill* (erase) all characters from the cursor position to the end of the command line.
<Ctrl-l>	Redraw the screen.
<Ctrl-u>	Clear the entire line.
Other keys	Insert new characters at the cursor position.

Command Line Interface Shortcuts

Command Stacking

As a shortcut, you can type multiple commands on a single line, separated by forward slashes (**/**). You can connect as many commands as required to access the menu option that you want. For example, the keyboard shortcut to set the Stacking Master Interface address is as follows:

```
# /cfg/stack/mif/addr <IP address>
```

Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same menu or sub-menu. For example, the command shown above could also be entered as follows:

```
Main# c/st/m/a <IP address>
```

Tab Completion

By entering the first letter of a command at any menu prompt and hitting <*Tab*>, the CLI will display all commands or options in that menu that begin with that letter. Entering additional letters will further refine the list of commands or options displayed. If only one command fits the input text when <*Tab*> is pressed, that command will be supplied on the command line, waiting to be entered. If the <*Tab*> key is pressed without any input on the command line, the currently active menu will be displayed.

CHAPTER 4

The Information Menu

You can view configuration information for the switch in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch information.

/info Information Menu

```
[Information Menu]
     sys      - System Information Menu
     stack    - Stacking Menu
     l2       - Layer 2 Information Menu
     l3       - Layer 3 Information Menu
     qos      - QoS Menu
     acl      - Show ACL information
     link     - Show link status
     port     - Show port information
     transcvr - Show Port Transceiver status
     dump     - Dump all information
```

The information provided by each menu option is briefly described in Table 4-1, with pointers to detailed information.

Table 4-1 Information Menu Options (/info)

Command Syntax and Usage
sys Displays the System Information Menu. For details, see page 35.
l2 Displays the Layer 2 Information Menu. For details, see page 50.

Table 4-1 Information Menu Options (/info)

Command Syntax and Usage
l3 Displays the Layer 3 Information Menu. For details, see page 59.
qos Displays the Quality of Service (QoS) Information Menu. For details, see page 67.
acl Displays the current configuration profile for each Access Control List (ACL) and ACL Group. For details, see page 69.
link Displays configuration information about each port, including: ■ Port alias and number ■ Port speed ■ Duplex mode (half, full, or auto) ■ Flow control for transmit and receive (no or yes) ■ Link status (up, down or disabled) For details, see page 70.
port Displays port status information, including: ■ Port alias and number ■ Whether the port uses VLAN Tagging or not ■ Port VLAN ID (PVID) ■ Port name ■ VLAN membership For details, see page 71.
transcvr Displays the status of the port transceiver module on each Fiber External Port. For details, see page 72.
dump Dumps all switch information available from the Information Menu (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

/info/sys
System Information

```
[System Menu]
     snmpv3    - SNMPv3 Information Menu
     general   - Show general system information
     log       - Show last 100 syslog messages
     user      - Show current user status
     dump      - Dump all system information
```

The information provided by each menu option is briefly described in Table 4-2, with pointers to where detailed information can be found.

Table 4-2 System Menu Options (/info/sys)

Command Syntax and Usage
snmpv3 Displays SNMPv3 Information Menu. To view the menu options, see page 36.
general Displays system information, including: ■ System date and time ■ Switch model name and number ■ Switch name and location ■ Time of last boot ■ MAC address of the switch management processor ■ IP address of the management interface ■ Hardware version and part number ■ Software image file and version number ■ Configuration name ■ Log-in banner, if one is configured For details, see page 46.
log Displays most recent syslog messages. For details, see page 47.
user Displays configured user names and their status. For details, see page 47.
dump Dumps all switch information available from the Information Menu (10K or more, depending on your configuration).

/info/sys/snmpv3
SNMPv3 System Information Menu

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC2271 to RFC2276.

```
[SNMPv3 Information Menu]
     usm       - Show usmUser table information
     view      - Show vacmViewTreeFamily table information
     access    - Show vacmAccess table information
     group     - Show vacmSecurityToGroup table information
     comm      - Show community table information
     taddr     - Show targetAddr table information
     tparam    - Show targetParams table information
     notify    - Show notify table information
     dump      - Show all SNMPv3 information
```

Table 4-3 SNMPv3 information Menu Options (/info/sys/snmpv3)

Command Syntax and Usage
usm Displays User Security Model (USM) table information. To view the table, see page 38.
view Displays information about view, sub-trees, mask and type of view. To view a sample, see page 39.
access Displays View-based Access Control information. To view a sample, see page 40.
group Displays information about the group that includes, the security model, user name, and group name. To view a sample, see page 41.
comm Displays information about the community table information. To view a sample, see page 41.
taddr Displays the Target Address table information. To view a sample, see page 42.

Table 4-3 SNMPv3 information Menu Options (/info/sys/snmpv3)

Command Syntax and Usage
tparam Displays the Target parameters table information. To view a sample, see page 43.
notify Displays the Notify table information. To view a sample, see page 44.
dump Displays all the SNMPv3 information. To view a sample, see page 45.

/info/sys/snmpv3/usm

SNMPv3 USM User Table Information

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. The USM user table contains the following information:

- the user name
- a security name in the form of a string whose format is independent of the Security Model
- an authentication protocol, which is an indication that the messages sent on behalf of the user can be authenticated
- the privacy protocol

```
usmUser Table:
User Name                       Protocol
------------------------------- -------------------------------
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH,  NO PRIVACY
```

Table 4-4 USM User Table Information Parameters (/info/sys/usm)

Field	Description
`User Name`	This is a string that represents the name of the user that you can use to access the switch.
`Protocol`	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. BLADE OS supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA.

/info/sys/snmpv3/view
SNMPv3 View Table Information

The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group's rights in terms of a particular MIB view for security reasons.

```
View Name            Subtree                Mask          Type
-----------------    -----------------   -------------  --------
iso                  1.3                                 included
v1v2only             1.3                                 included
v1v2only             1.3.6.1.6.3.15                      excluded
v1v2only             1.3.6.1.6.3.16                      excluded
v1v2only             1.3.6.1.6.3.18                      excluded
```

Table 4-5 SNMPv3 View Table Information Parameters (/info/sys/snmpv3/view)

Field	Description
`View Name`	Displays the name of the view.
`Subtree`	Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names.
`Mask`	Displays the bit mask.
`Type`	Displays whether a family of `view subtrees` is included or excluded from the MIB view.

/info/sys/snmpv3/access

SNMPv3 Access Table Information

The access control sub system provides authorization services.

The vacmAccessTable maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

```
Group Name Prefix Model   Level       Match  ReadV   WriteV   NotifyV
---------- ------ ------- ------      ------ ------  ------   -------
v1v2grp           snmpv1  noAuthNoPriv exact  iso      iso    v1v2only
admingrp           usm     authPriv     exact  iso      iso        iso
```

Table 4-6 SNMPv3 Access Table Information (/info/sys/snmpv3/access)

Field	Description
`Group Name`	Displays the name of group.
`Prefix`	Displays the prefix that is configured to match the values.
`Model`	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
`Level`	Displays the minimum level of security required to gain rights of access. For example, `noAuthNoPriv`, `authNoPriv`, or `authPriv`.
`Match`	Displays the match for the contextName. The options are: `exact` and `prefix`.
`ReadV`	Displays the MIB view to which this entry authorizes the read access.
`WriteV`	Displays the MIB view to which this entry authorizes the write access.
`NotifyV`	Displays the Notify view to which this entry authorizes the notify access.

/info/sys/snmpv3/group
SNMPv3 Group Table Information

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

```
Sec Model    User Name                       Group Name
----------   ------------------------------  --------------------
snmpv1       v1v2only                        v1v2grp
usm          adminmd5                        admingrp
usm          adminsha                        admingrp
```

Table 4-7 SNMPv3 Group Table Information Parameters (/info/sys/snmpv3/group)

Field	Description
Sec Model	Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3.
User Name	Displays the name for the group.
Group Name	Displays the access name of the group.

/info/sys/snmpv3/comm
SNMPv3 Community Table Information

This command displays the community table information stored in the SNMP engine.

```
Index      Name       User Name           Tag
---------- ---------- ------------------- ----------
trap1      public     v1v2only            v1v2trap
```

Table 4-8 SNMPv3 Community Table Parameters (/info/sys/snmpv3/comm)

Field	Description
Index	Displays the unique index value of a row in this table
Name	Displays the community string, which represents the configuration.
User Name	Displays the User Security Model (USM) user name.
Tag	Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap.

/info/sys/snmpv3/taddr

SNMPv3 Target Address Table Information

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

```
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------
trap1      47.81.25.66     162  v1v2trap   v1v2param
```

Table 4-9 SNMPv3 Target Address Table Information Parameters (/info/sys/snmpv3/taddr)

Field	Description
`Name`	Displays the locally arbitrary, but unique identifier associated with this `snmpTargetAddrEntry`.
`Transport Addr`	Displays the transport addresses.
`Port`	Displays the SNMP UDP port number.
`Taglist`	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
`Params`	The value of this object identifies an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

/info/sys/snmpv3/tparam

SNMPv3 Target Parameters Table Information

```
Name            MP Model   User Name          Sec Model  Sec Level
--------------- --------   --------------     ---------  ---------
v1v2param       snmpv2c    v1v2only           snmpv1     noAuthNoPriv
```

Table 4-10 SNMPv3 Target Parameters Table Information (/info/sys/snmpv3/tparam)

Field	Description
`Name`	Displays the locally arbitrary, but unique identifier associated with this `snmpTargeParamsEntry`.
`MP Model`	Displays the Message Processing Model used when generating SNMP messages using this entry.
`User Name`	Displays the `securityName`, which identifies the entry on whose behalf SNMP messages will be generated using this entry.
`Sec Model`	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an `inconsistentValue` error if an attempt is made to set this variable to a value for a security model which the system does not support.
`Sec Level`	Displays the level of security used when generating SNMP messages using this entry.

/info/sys/snmpv3/notify

SNMPv3 Notify Table Information

```
Name                 Tag
-------------------- --------------------
v1v2trap             v1v2trap
```

Table 4-11 SNMPv3 Notify Table Information (/info/sys/snmpv3/notify)

Field	Description
Name	The locally arbitrary, but unique identifier associated with this snmpNotifyEntry.
Tag	This represents a single tag value which is used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable that contains a tag value equal to the value of this entry, is selected. If this entry contains a value of zero length, no entries are selected.

/info/sys/snmpv3/dump

SNMPv3 Dump Information

```
usmUser Table:
User Name                       Protocol
------------------------------- -------------------------------
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH,  NO PRIVACY

vacmAccess Table:
Group Name Prefix Model   Level        Match ReadV   WriteV  NotifyV
---------- ------ ------- ---------- ------ ------- --------  ------
v1v2grp          snmpv1  noAuthNoPriv exact  iso     iso     v1v2only
admingrp          usm     authPriv     exact  iso     iso     iso

vacmViewTreeFamily Table:
View Name            Subtree           Mask            Type
-------------------- ---------------  ------------    --------------
iso                  1.3                               included
v1v2only             1.3                               included
v1v2only             1.3.6.1.6.3.15                    excluded
v1v2only             1.3.6.1.6.3.16                    excluded
v1v2only             1.3.6.1.6.3.18                    excluded

vacmSecurityToGroup Table:
Sec Model  User Name                       Group Name
---------- -------------------------------  ------------------------
snmpv1     v1v2only                        v1v2grp
usm        adminsha                        admingrp

snmpCommunity Table:
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------
snmpNotify Table:
Name                 Tag
-------------------- --------------------
snmpTargetAddr Table:
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------
snmpTargetParams Table:
Name                MP Model User Name           Sec Model Sec Level
------------------- -------- ------------------  --------- -------
```

/info/sys/general
General System Information

```
Blade Network Technologies Rack Switch G8000

System Information at
 Sun Jan 15 23:56:24 2009
 Switch has been up for 0 day, 0 hour, 19 minutes and 31 seconds
Last boot:(power cycle)

MAC address: 00:18:b1:8a:36:00    IP (If 1) address: 172.24.1.70
Revision: 8
Switch Serial No: US38200028
Spare Part No: BAC-00017-00
Manufacturing date: 08/20
Software Version 6.0.1 (FLASH image2), active configuration.

Fans are in Forward AirFlow, Warning at 55 C and Recover at 80 C

Temperature Sensor 1:   32.0 C
Temperature Sensor 2:   38.0 C
Temperature Sensor 3: --.-
Temperature Sensor 4:   31.0 C
Speed of Fan 1: 0 RPM
Speed of Fan 2: 0 RPM
Speed of Fan 3: 0 RPM
Speed of Fan 4: 4224 RPM
Speed of Fan 5: 6272 RPM

State of Power Supply 1:   On
State of Power Supply 2:   Off
```

NOTE – The display of temperature will come up only if the temperature of any of the sensors exceeds the temperature threshold. There will be a warning from the software if any of the sensors exceeds this temperature threshold. The switch will shut down if the power supply overheats.

System information includes:

- System date and time
- Switch model
- Switch name and location
- Time of last boot
- MAC address of the switch management processor
- IP address of IP interface 128

- Hardware version and part number
- Software image file and version number
- Configuration name
- Log-in banner, if one is configured

/info/sys/log
Show Recent Syslog Messages

```
Jan 26 2008 18:03:27 RS G8000:CLI-ALERT:User (admin) logged in on console
Jan 26 2008 18:07:32 RS G8000:CFA-NOTICE:system: link up on port 2:2
Jan 26 2008 18:11:12 RS G8000:SYSTEM-CRITICAL:Warning: Fan Failure
```

/info/sys/user
User Status

```
Usernames:
  user      - enabled - offline
  oper      - disabled - offline
  admin     - Always Enabled - online 1 session
Current User ID table:
  1: name paul    , dis, cos user     , password valid, offline
Current strong password settings:
  strong password status: disabled
```

This command displays the status of the configured usernames.

/info/stack
Stacking Information

```
[Stacking Menu]
     switch   - Show switch information
     link     - Show stack link information
     vers     - Show switch firmware information
     ip       - Show Master and Backup IP information
     path     - Show inter switch packet path map
     pushstat - Show config/image push status information
     dump     - Dump all stacking information
```

Table 4-12 lists the Stacking Information commands.

Table 4-12 Stacking Information menu (/info/stack)

Command Syntax and Usage
switch Displays information about each switch in the stack, including: ■ Configured Switch Number (csnum) ■ Assigned Switch Number (asnum) ■ MAC address ■ Stacking state
link Displays link information for each switch in the stack.
vers Displays the firmware version number for the selected switch.
ip Displays the IP address and gateway of the Master Switch Interface and the Backup Switch Interface.
path Displays the Stacking packet path map that shows how the stack switches are connected.
pushstat Displays the status of the most recent firmware and configuration file push from the master to member switches.
dump Displays all stacking information.

info/stack/switch

Show Stacking Switch Information

```
Stack name: Stack1
Local switch is the master.

Local switch:
   csnum             - 1
   MAC               - 00:22:00:ac:bd:00
   Switch Type       - 9
   Chassis Type      - 99
   Switch Mode (cfg) - Master
   Priority          - 225
   Stack MAC         - 00:22:00:ac:bd:1f

Master switch:
   csnum             - 1
   MAC               - 00:22:00:ac:bd:00

Backup switch:
   csnum             - 3
   MAC               - 00:00:60:10:00:00

Configured Switches:
-------------------------------------
csnum           MAC           asnum
-------------------------------------
 C1     00:22:00:ac:bd:00    A1
 C2     00:00:00:00:00:00
 C3     00:00:60:10:00:00    A2

Attached Switches in Stack:
---------------------------------------------
asnum           MAC           csnum  State
---------------------------------------------
 A1     00:22:00:ac:bd:00     C1    IN_STACK
 A2     00:00:60:10:00:00     C3    IN_STACK
```

Stack switch information includes the following:

- Details about the local switch from which the command was issued
- Configured switch number and MAC of the Stack Master and Backup
- Configured switch numbers and their associate assigned switch numbers
- Assigned switch numbers and their associate configured switch numbers

/info/l2
Layer 2 Information

```
[Layer 2 Menu]
     fdb      - Forwarding Database Information Menu
     lacp     - Link Aggregation Control Protocol Menu
     failovr  - Show Failover information
     8021x    - Show 802.1x information
     bpdugrd  - Show BPDU Guard information
     trunk    - Show Trunk Group information
     vlan     - Show VLAN information
     dump     - Dump all layer 2 information
```

The information provided by each menu option is briefly described in Table 4-13, with pointers to where detailed information can be found.

Table 4-13 Layer 2 Menu Options (/info/l2)

Command Syntax and Usage
fdb Displays the Forwarding Database Information Menu. For details, see page 51.
lacp Displays the Link Aggregation Control Protocol Menu. For details, see page 53.
failovr Displays the Layer 2 Failover Information Menu. For details, see page 54.
8021x Displays the 802.1X Information Menu. For details, see page 56.
bpdugrd Displays the status of BPDU Guard.
trunk When trunk groups are configured, you can view the state of each port in the various trunk groups. For details, see page 57.
vlan Displays VLAN configuration information, including: ■ VLAN Number ■ VLAN Name ■ Status ■ Port membership of the VLAN For details, see page 58.

Table 4-13 Layer 2 Menu Options (/info/l2)

Command Syntax and Usage
dump Dumps all switch information available from the Layer 2 menu (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

/info/l2/fdb
FDB Information

```
[Forwarding Database Menu]
      find    - Show a single FDB entry by MAC address
      port    - Show FDB entries on a single port
      trunk   - Show FDB entries on a single trunk
      vlan    - Show FDB entries on a single VLAN
      state   - Show FDB entries by state
      dump    - Show all FDB entries
```

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

NOTE – The master forwarding database supports up to 16K MAC address entries on the MP per switch.

Table 4-14 FDB Information Menu Options (/info/l2/fdb)

Command Syntax and Usage
find *<MAC address>* [*<VLAN>*] Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56`. You can also enter the MAC address using the format, `xxxxxxxxxxxx`. For example, `080020123456`.
port *<port number or alias>* Displays all FDB entries for a particular port.
trunk *<trunk number>* Displays all FDB entries for a particular trunk group.

Table 4-14 FDB Information Menu Options (/info/l2/fdb)

Command Syntax and Usage
vlan *<VLAN number (1-4095)>* Displays all FDB entries on a single VLAN.
state unknown|forward|trunk| Displays all FDB entries of a particular state.
dump Displays all entries in the Forwarding Database. For more information, see page 52.

/info/l2/fdb/dump
Show All FDB Information

```
    MAC address      VLAN  Port  Trnk  State  Permanent
-----------------  ----  ----  ----  -----  ---------
00:04:38:90:54:18     1  4             FWD
00:09:6b:9b:01:5f     1  13            FWD
00:09:6b:ca:26:ef     1  22            FWD
00:0f:06:ec:3b:00     1  35            FWD
00:11:43:c4:79:83     1  4             FWD
00:11:f9:36:71:00     1  22            FWD
00:13:0a:4d:3c:00     1  35            FWD       P
```

An address that is in the forwarding (FWD) state, means that it has been learned by the switch. When in the trunking (TRK) state, the port field represents the trunk group number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address. When an address is in the unknown state, no outbound port is indicated, although ports which reference the address as a destination will be listed under "Reference ports."

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to "Forwarding Database Maintenance" on page 220.

/info/l2/lacp
Link Aggregation Control Protocol Information

```
[LACP Menu]
     aggr      - Show LACP aggregator information for the port
     port      - Show LACP port information
     dump      - Show all LACP ports information
```

Use these commands to display Link Aggregation Protocol (LACP) status information about each port on the G8000.

Table 4-15 LACP Menu Options (/info/l2/lacp)

Command Syntax and Usage
aggr Displays detailed information of the LACP aggregator used by the selected port.
port Displays LACP information about the selected port.
dump Displays a summary of LACP information. For details, see page 53.

/info/l2/lacp/dump
Show all LACP Information

```
port  lacp   adminkey  operkey  selected  prio    attached  trunk
                                                    aggr
------------------------------------------------------------------
1     active     30       30         y     32768      17      19
2     active     30       30         y     32768      17      19
3     off        19       19         n     32768      --      --
4     off        20       20         n     32768      --      --
...
```

LACP dump includes the following information for each external port in the G8000:

- lacp
  Displays the port's LACP mode (active, passive, or off)
- adminkey
  Displays the value of the port's *adminkey*.
- operkey
  Shows the value of the port's operational key.

- selected
  Indicates whether the port has been selected to be part of a Link Aggregation Group.
- prio
  Shows the value of the port priority.
- attached aggr
  Displays the aggregator associated with each port.
- trunk
  This value represents the LACP trunk group number.

/info/l2/failovr
Layer 2 Failover Information Menu

```
[Failover Info Menu]
     trigger  - Show Trigger information
```

Table 4-16 describes the Layer 2 Failover information options.

Table 4-16 Failover Menu Options (/info/l2/failovr)

Command Syntax and Usage
trigger *<trigger number>* Displays detailed information about the selected Layer 2 Failover trigger.

/info/l2/failovr/trigger <trigger number>

Show Layer 2 Failover Information

```
Trigger 1 Auto Monitor: Enabled
Trigger 1 limit: 0
Monitor State: Up
Member      Status
---------   -----------
trunk 1
 2:2       Operational
 2:3       Operational

Control State: Auto Disabled
Member      Status
---------   -----------
 1:1       Operational
 1:2       Operational
 1:3       Operational
 1:4       Operational
...
```

The Layer 2 Failover trigger information includes the following:

- Monitor status (enabled or disabled)
- Trigger limit
- Monitor state (up or down)
- Monitor members and status of each member (operational or failed)
- Control members and status of each member (operational or failed)

/info/l2/8021x
802.1X Information

```
System capability : Authenticator
System status     : enabled
Protocol version  : 1
Guest VLAN status : disabled
Guest VLAN        : none
                                    Authenticator    Backend   Assigned
Port    Auth Mode    Auth Status      PAE State     Auth State   VLAN
-----  ------------  ------------  --------------  ---------- ------
*1:1   force-auth    unauthorized  initialize      initialize   none
*1:2   force-auth    unauthorized  initialize      initialize   none
*1:3   force-auth    unauthorized  initialize      initialize   none
*1:4   force-auth    unauthorized  initialize      initialize   none
*1:5   force-auth    unauthorized  initialize      initialize   none
*1:6   force-auth    unauthorized  initialize      initialize   none
*1:7   force-auth    unauthorized  initialize      initialize   none
*1:8   force-auth    unauthorized  initialize      initialize   none
*1:9   force-auth    unauthorized  initialize      initialize   none
*1:10  force-auth    unauthorized  initialize      initialize   none
*1:11  force-auth    unauthorized  initialize      initialize   none
*1:12  force-auth    unauthorized  initialize      initialize   none
...
------------------------------------------------------------------------
* - Port down or disabled
```

The following table describes the IEEE 802.1X parameters.

Table 4-17 802.1X Parameter Descriptions (/info/l2/8021x)

Parameter	Description
Port	Displays each port's alias.
`Auth Mode`	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: ■ force-unauth ■ auto ■ force-auth
`Auth Status`	Displays the current authorization status of the port, either authorized or unauthorized.

Table 4-17 802.1X Parameter Descriptions (Continued)(/info/l2/8021x)

Parameter	Description
`Authenticator PAE State`	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: ■ initialize ■ disconnected ■ connecting ■ authenticating ■ authenticated ■ aborting ■ held ■ forceAuth
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: ■ initialize ■ request ■ response ■ success ■ fail ■ timeout ■ idle
Assigned VLAN	Displays the VLAN assigned to the port, if applicable.

/info/l2/trunk
Trunk Group Information

```
Trunk group 1: Enabled
Protocol - Static
Port State:
  2:2: detached
  2:3: detached
```

When trunk groups are configured, you can view the state of each port in the various trunk groups.

/info/l2/vlan
VLAN Information

```
VLAN                Name                 Status            Ports
----  -------------------------------  ------  --------------------
1     Default VLAN                       ena     1:1-1:50 2:1-2:50 3:1-3:50
                                                 4:1-4:50 5:1-5:50 6:1-6:50
20    VLAN 20                            ena     empty
30    VLAN 30                            ena     empty
4090  STK VLAN                          ena     1:51 1:52 2:51 2:52 3:51 3:52
                                                 4:51 4:52 5:51 5:52 6:51 6:52
```

This information display includes all configured VLANs and all member ports that have an active link state. Port membership is represented in slot/port format.

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN

/info/l3
Layer 3 Information

```
[Layer 3 Menu]
     arp       - ARP Information Menu
     igmp      - Show IGMP Snooping Multicast Group information
     ip        - Show IP information
     dump      - Dump all layer 3 information
```

The information provided by each menu option is briefly described in Table 4-18, with pointers to detailed information.

Table 4-18 Layer 3 Menu Options (/info/l3)

Command Syntax and Usage
arp Displays the Address Resolution Protocol (ARP) Information Menu. For details, see page 61.
igmp Displays IGMP Information Menu. For details, see page 63.
ip Displays IP Information. For details, see page 63.
dump Dumps all switch information available from the Layer 3 Menu (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

/info/l3/dump
Layer 3 Information

```
Interface information:
   1: 10.1.1.1          255.255.0.0         10.1.1.255,vlan1, up

Default gateway information:
  10.1.1.2, enabled,  active

Master switch IP interface configured through DHCP
MAC address:         00:22:00:ac:bd:1f
IP address:          127.31.37.158
Subnet mask:         255.255.0.0
Default gateway:     127.31.1.1
DHCP Server:         127.31.35.1
Lease Obtained:      11:35:44 Mon Aug  3, 2009
Lease Expires:       14:31:40 Mon Aug 10, 2009

Current ARP configuration:
rearp 5
ARP cache information:

IP Address       Flags     Hardware Address    Interface
--------------   ------    -----------------   ---------
10.1.1.1                   00:15:40:07:20:42    1

Route table information:
Status code: * - best
Destination      Mask            Gateway          Type      Tag         Metr  If
---------------  --------------- ---------------- ----------- ---------- ---- ---
* 10.1.1.0        255.255.255.0    0.0.0.0          direct     fixed           1
* 10.1.1.1        255.255.255.255  10.1.1.1         local      addr       0    1
* 10.1.1.255      255.255.255.255  10.1.1.255       bcast      bcast      0    1
```

/info/l3/arp
ARP Information

```
[Address Resolution Protocol Menu]
      find    - Show a single ARP entry by IP address
      port    - Show ARP entries on a single port
      vlan    - Show ARP entries on a single VLAN
      dump    - Show all ARP entries
      addr    - Show ARP address list
```

The ARP information includes IP address and MAC address of each entry, address status flags (see Table 4-19 on page 61), VLAN and port for the address, and port referencing information.

Table 4-19 ARP Information Menu Options (/info/l3/arp)

Command Syntax and Usage
find *<IP address (such as, 192.4.17.101>* Displays a single ARP entry by IP address.
port *<port number>* Displays the ARP entries on a single port.
vlan *<VLAN number (1-4095)>* Displays the ARP entries on a single VLAN.
dump Displays all ARP entries. including: ■ IP address and MAC address of each entry ■ Address status flag (see below) ■ The VLAN and port to which the address belongs ■ The ports which have referenced the address (empty if no port has routed traffic to the IP address shown) For more information, see page 62.
addr Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.

/info/l3/arp/dump

Show All ARP Entry Information

```
IP address     Flags    MAC address       VLAN  Port
-------------- ----- ----------------- ---- ----
47.80.22.1            00:e0:16:7c:28:86    1  1:6
47.80.23.243     P    00:03:42:fa:3b:30    1
47.80.23.245          00:c0:4f:60:3e:c1    1  1:6
190.10.10.1      P    00:03:42:fa:3b:30   10
```

NOTE – If you have VMA turned on, the referenced port will be the designated port. If you have VMA turned off, the designated port will be the normal ingress port.

The `Flag` field is interpreted as follows:

Table 4-20 ARP Dump Flag Parameters

Flag	Description
`P`	Permanent entry created for switch IP interface.
`R`	Indirect route entry.
`U`	Unresolved ARP entry. The MAC address has not been learned.

/info/l3/arp/addr

ARP Address List Information

```
  IP address        IP mask         MAC address     VLAN Flags
-------------- --------------- ----------------- ---- -----
205.178.18.66   255.255.255.255  00:70:cf:03:20:04        P
205.178.50.1    255.255.255.255  00:70:cf:03:20:06    1
205.178.18.64   255.255.255.255  00:70:cf:03:20:05    1
```

/info/l3/igmp
IGMP Multicast Group Information

```
[IGMP Multicast Menu]
     mrouter  - Show IGMP Snooping Multicast Router Port information
     find     - Show a single group by IP group address
     vlan     - Show groups on a single vlan
     port     - Show groups on a single port
     trunk    - Show groups on a single trunk
     detail   - Show detail of a single group by IP group address
     dump     - Show all groups
```

Table 4-21 describes the commands used to display information about IGMP groups learned by the switch.

Table 4-21 IGMP Multicast Group Information Menu Options (/info/l3/igmp)

Command Syntax and Usage
mrouter Displays IGMP Multicast Router menu. To view menu options, see page 64.
find *<IP address>* Displays a single IGMP multicast group by its IP address.
vlan *<VLAN number>* Displays all IGMP multicast groups on a single VLAN.
port *<port number or alias>* Displays all IGMP multicast groups on a single port.
trunk *<trunk number>* Displays all IGMP multicast groups on a single trunk group.
detail *<IP address>* Displays details about IGMP multicast groups, including source and timer information.
dump Displays information for all multicast groups.

info/l3/igmp/dump
IGMP Group Information

```
Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.
     Group        VLAN     Port    Version    Expires
--------------- ------- ------ --------    -------
226.0.0.0        1        1:18    V2         3:19
226.0.0.1        1        1:18    V2         3:19
226.0.0.2        1        1:18    V2         3:19
226.0.0.3        1        1:18    V2         3:19
226.0.0.4        1        1:18    V2         3:19
```

IGMP Group information includes:

- IGMP Group address
- VLAN and port
- IGMP version
- Expiration timer value

/info/l3/igmp/mrouter
IGMP Multicast Router Port Information

```
[IGMP Multicast Router Menu]
     vlan     - Show all multicast router ports on a single vlan
     dump     - Show all learned multicast router ports
```

Table 4-22 describes the commands used to display information about multicast routers (Mrouters) learned through IGMP Snooping.

Table 4-22 IGMP Mrouter Information Menu Options (/info/igmp/mrouter)

Command Syntax and Usage
vlan *<VLAN number>* Displays the multicast router ports configured or learned on the selected VLAN.
dump Displays information for all multicast groups learned by the switch.

info/l3/igmp/mrouter/dump
IGMP Mrouter Information

```
SrcIP               VLAN      Port      Version    Expires    MRT
------------------- -------   -------   ---------  --------   -------
10.10.254.10         1         5:44       V2       3:59      10
```

IGMP Mrouter information includes:

- Source IP address
- VLAN number
- Port number
- IGMP version
- Expiration time

/info/l3/ip
IP Information

```
Interface information:

1: 10.200.30.3  255.255.255.0   3.3.3.255,     vlan 1, up

Default gateway information: metric strict
  1: 10.200.1.1,     vlan any,  up

Master switch IP interface configured through DHCP
MAC address:        00:22:00:ac:bd:1f
IP address:         12.31.37.158
Subnet mask:        255.255.0.0
Default gateway:    12.31.1.1
DHCP Server:        12.31.35.1
Lease Obtained:     11:00:18 Mon Aug 10, 2009
Lease Expires:      20:12:37 Tue Aug 11, 2009
```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask/prefix, broadcast address, VLAN number, and operational status.
- Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status.
- Stacking Master Interface information.

/info/qos
Quality of Service Information

```
[QoS Menu]
     8021p    - Show QOS 802.1p information
```

Table 4-23 QoS Menu Options (/info/qos)

Command Syntax and Usage
8021p Displays the 802.1p Information Menu. For details, see page 67.

/info/qos/8021p
802.1p Information

```
Current priority to COS queue information:
Priority  COSq  Weight
--------  ----  ------
    0       0       1
    1       0       1
    2       0       1
    3       0       1
    4       0       1
    5       0       1
    6       0       1
    7       1       4

Current port priority information:
Port   Priority  COSq  Weight
-----  --------  ----  ------
1:1         0       0       1
1:2         0       0       1
...

2:1         0       0       1
2:2         0       0       1
2:3         0       0       1
2:4         0       0       1
...
```

The following table describes the IEEE 802.1p priority to COS queue information.

Table 4-24 802.1p Priority-to-COS Queue Parameter Descriptions

Parameter	Description
Priority	Displays the 802.1p Priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight of the COS queue.

The following table describes the IEEE 802.1p port priority information.

Table 4-25 802.1p Port Priority Parameter Descriptions

Parameter	Description
Port	Displays the port alias.
Priority	Displays the 802.1p Priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight.

info/acl
Access Control List Information

```
Current ACL information:
------------------------
  Filter 2 profile:
   Ethernet
     - VID        : 2/0xfff
   Meter
     - Set to disabled
     - Set committed rate : 64
     - Set max burst size : 32
   Re-Mark
     - Set use of TOS precedence to disabled
   Actions        : Permit
  No ACL groups configured.
```

Access Control List (ACL) information includes configuration settings for each ACL and ACL Group.

Table 4-26 ACL Parameter Descriptions

Parameter	Description
`Filter x profile`	Indicates the ACL number.
`Meter`	Displays the ACL meter parameters.
`Re-Mark`	Displays the ACL re-mark parameters.
`Actions`	Displays the configured action for the ACL.

/info/link
Link Status Information

```
RS G8000(config)# show interface link
------------------------------------------------------------------------
Alias   Port   Speed    Duplex     Flow Ctrl      Link
-----   ----   -----   --------  --TX-----RX--   ------
1:1      65      any      any     yes    yes      down
1:2      66      any      any     yes    yes      down
1:3      67      any      any     yes    yes      down
1:4      68      any      any     yes    yes      down
1:5      69      any      any     yes    yes      down
1:6      70      any      any     yes    yes      down
1:7      71      any      any     yes    yes      down
1:8      72      any      any     yes    yes      down
1:9      73      any      any     yes    yes      down
1:10     74      any      any     yes    yes      down
1:11     75      any      any     yes    yes      down
1:12     76      any      any     yes    yes      down
1:13     77      any      any     yes    yes      down
1:14     78      any      any     yes    yes      down
1:15     79      any      any     yes    yes      down
1:16     80      any      any     yes    yes      down
1:17     81      any      any     yes    yes      down
1:18     82      any      any     yes    yes      down
1:19     83      any      any     yes    yes      down
1:20     84      any      any     yes    yes      down
...
```

Port link information includes the following:

- Port alias and number
- Port speed (10, 100, 1000, 10000, or any)
- Duplex mode (half, full, or any)
- Flow control for transmit and receive (no or yes)
- Link status (up, down, or disabled)

/info/port
Port Information

```
Alias Port Tag    Type     PVID       NAME                    VLAN(s)
----- ---- --- ---------- ----- -------------- ----------------------
1:1   65    n  External      1* External1:1    1
1:2   66    n  External      1* External1:2    1
1:3   67    n  External      1* External1:3    1
1:4   68    n  External      1* External1:4    1
1:5   69    n  External      1* External1:5    1
1:6   70    n  External      1* External1:6    1
1:7   71    n  External      1* External1:7    1
1:8   72    n  External      1* External1:8    1
1:9   73    n  External      1* External1:9    1
1:10  74    n  External      1* External1:10   1
...
# = PVID is tagged.
```

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (`y` or `n`)
- Port VLAN ID (**`PVID`**)
- Port name
- VLAN membership

/info/transcvr
Fiber Port Transceiver Status

```
Modules:
Switch   IO Module         Type         Part Number              Serial
------  ------------   ------------   ----------------       ----------------
1       Front module    Not inserted
1       Rear module     CX4             BAC-00027-00            CH4825008X
```

/info/dump
Information Dump

Use the dump command to dump all switch information available from the Information Menu (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

CHAPTER 5

The Statistics Menu

You can view switch performance statistics in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch statistics.

/stats
Statistics Menu

```
[Statistics Menu]
     port      - Port Stats Menu
     l2        - Layer 2 Stats Menu
     l3        - Layer 3 Stats Menu
     mp        - MP-specific Stats Menu
     acl       - ACL Stats Menu
     snmp      - Show SNMP stats
     ntp       - Show NTP stats
     clrmp     - Clear all MP related stats
     clrports  - Clear stats for all ports
     dump      - Dump all stats
```

The information provided by each menu option is briefly described in Table 5-1, with pointers to detailed information.

Table 5-1 Statistics Menu Options (/stats)

Command Syntax and Usage
port *<port number>* Displays the Port Statistics Menu for the specified port. Use this command to display traffic statistics on a port-by-port basis. Traffic statistics are included in SNMP Management Information Base (MIB) objects. To view menu options, see page 75.
l2 Displays the Layer 2 Stats Menu. To view menu options, see page 87.
l3 Displays the Layer 3 Stats Menu. To view menu options, see page 89.
mp Displays the Management Processor Statistics Menu. Use this command to view information on how switch management processes and resources are currently being allocated. To view menu options, see page 100.
acl Displays ACL Statistics menu. To view menu options, see page 104.
snmp Displays SNMP statistics. See page 105 for sample output.
ntp [clear] Displays Network Time Protocol (NTP) Statistics. See page 109 for a sample output and a description of NTP Statistics. Use the following command to clear all NTP statistics: `ntp clear`
clrmp Clears all management processor statistics.
clrports Clears statistics counters for all ports.
dump Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. For details, see page 110.

/stats/port <port number>
Port Statistics

This menu displays traffic statistics on a port-by-port basis. Traffic statistics include SNMP Management Information Base (MIB) objects.

```
[Port Statistics Menu]
     8021x    - Show 802.1X stats
     brg      - Show bridging ("dot1") stats
     ether    - Show Ethernet ("dot3") stats
     if       - Show interface ("if") stats
     ip       - Show Internet Protocol ("IP") stats
     link     - Show link stats
     dump     - Show all port stats
     clear    - Clear all port stats
```

Table 5-2 Port Statistics Menu Options (/stats/port)

Command Syntax and Usage
8021x Displays IEEE 802.1X statistics for the port. See page 77 for sample output.
brg Displays bridging (“dot1”) statistics for the port. See page 79 for sample output.
ether Displays Ethernet (“dot3”) statistics for the port. See page 81 for sample output.
if Displays interface statistics for the port. See page 84 for sample output.
ip Displays IP statistics for the port. See page 86 for sample output.
link Displays link statistics for the port. See page 86 for sample output.
dump Displays all port statistics.
clear This command clears all the statistics on the port.

/stats/port <port number>/8021x
802.1X Authenticator Statistics

This menu option enables you to display the 802.1X authenticator statistics of the selected port.

```
Authenticator Statistics:
  eapolFramesRx          = 925
  eapolFramesTx          = 3201
  eapolStartFramesRx     = 2
  eapolLogoffFramesRx    = 0
  eapolRespIdFramesRx    = 463
  eapolRespFramesRx      = 460
  eapolReqIdFramesTx     = 1820
  eapolReqFramesTx       = 1381
  invalidEapolFramesRx   = 0
  eapLengthErrorFramesRx = 0
  lastEapolFrameVersion  = 1
  lastEapolFrameSource   = 00:01:02:45:ac:51
```

Table 5-3 802.1X Authenticator Statistics of a Port (/stats/port/8021x)

Statistics	Description
eapolFramesRx	Total number of EAPOL frames received
eapolFramesTx	Total number of EAPOL frames transmitted
eapolStartFramesRx	Total number of EAPOL Start frames received
eapolLogoff-FramesRx	Total number of EAPOL Logoff frames received
eapolRespId-FramesRx	Total number of EAPOL Response Identity frames received
eapolRespFramesRx	Total number of Response frames received
eapolReqIdFramesTx	Total number of Request Identity frames transmitted
eapolReqFramesTx	Total number of Request frames transmitted
invalidEapol-FramesRx	Total number of invalid EAPOL frames received
eapLengthError-FramesRx	Total number of EAP length error frames received

Table 5-3 802.1X Authenticator Statistics of a Port (/stats/port/8021x)

Statistics	Description
lastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
lastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

/stats/port <port number>/8021x
802.1X Authenticator Diagnostics

This menu option enables you to display the 802.1X authenticator diagnostics of the selected port.

```
Authenticator Diagnostics:
  authEntersConnecting                 = 1820
  authEapLogoffsWhileConnecting        = 0
  authEntersAuthenticating             = 463
  authSuccessesWhileAuthenticating     = 5
  authTimeoutsWhileAuthenticating      = 0
  authFailWhileAuthenticating          = 458
  authReauthsWhileAuthenticating       = 0
  authEapStartsWhileAuthenticating     = 0
  authEapLogoffWhileAuthenticating     = 0
  authReauthsWhileAuthenticated        = 3
  authEapStartsWhileAuthenticated      = 0
  authEapLogoffWhileAuthenticated      = 0
  backendResponses                     = 923
  backendAccessChallenges              = 460
  backendOtherRequestsToSupplicant     = 460
  backendNonNakResponsesFromSupplicant = 460
  backendAuthSuccesses                 = 5
  backendAuthFails                     = 458
```

Table 5-4 802.1X Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
authEntersConnecting	Total number of times that the state machine transitions to the CONNECTING state from any other state.
authEapLogoffsWhileConnecting	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.

Table 5-4 802.1X Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
authEntersAuthenticating	Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
authSuccessesWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.
authTimeoutsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
authFailWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
authReauthsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request
authEapStartsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
authReauthsWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
backendResponses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
backendAccessChallenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.

Table 5-4 802.1X Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
backendOtherRequestsToSupplicant	Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method.
backendNonNakResponsesFromSupplicant	Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticator.s chosen EAP-method.
backendAuthSuccesses	Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
backendAuthFails	Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

/stats/port <port number>/brg
Bridging Statistics

This menu option enables you to display the bridging statistics of the selected port.

```
Bridging statistics for port 1:1:
dot1PortInFrames:                    63242584
dot1PortOutFrames:                   63277826
dot1PortInDiscards:                         0
dot1TpLearnedEntryDiscards:                 0
dot1StpPortForwardTransitions:              0
```

Table 5-5 Bridging Statistics of a Port (/stats/port/brg)

Statistics	Description
dot1PortInFrames	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortOutFrames	The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.

Table 5-5 Bridging Statistics of a Port (/stats/port/brg)

Statistics	Description
`dot1PortInDiscards`	Count of valid frames received which were discarded (that is, filtered) by the Forwarding Process.
`dot1TpLearnedEntry Discards`	The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
`dot1StpPortForward Transitions`	The number of times this port has transitioned from the Learning state to the Forwarding state.

/stats/port <port number>/ether
Ethernet Statistics

This menu option enables you to display the ethernet statistics of the selected port

```
Ethernet statistics for port 1:1:
dot3StatsAlignmentErrors:                    0
dot3StatsFCSErrors:                          0
dot3StatsSingleCollisionFrames:              0
dot3StatsMultipleCollisionFrames:            0
dot3StatsLateCollisions:                     0
dot3StatsExcessiveCollisions:                0
dot3StatsInternalMacTransmitErrors:         NA
dot3StatsFrameTooLongs:                      0
dot3StatsInternalMacReceiveErrors:           0
```

Table 5-6 Ethernet Statistics for Port (/stats/port/ether)

Statistics	Description
dot3StatsAlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsSingle-CollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollision-Frame object.

Table 5-6 Ethernet Statistics for Port (/stats/port/ether)

Statistics	Description
dot3StatsMultiple-CollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMul-ticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollision-Frames object.
dot3StatsLate-Collisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for pur-poses of other collision-related statistics.
dot3StatsExcessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternal-MacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3Stats-CarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.
dot3StatsFrameToo-Longs	A count of frames received on a particular interface that exceed the maxi-mum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error condi-tions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Table 5-6 Ethernet Statistics for Port (/stats/port/ether)

Statistics	Description
dot3StatsInternal-MacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3Stats-AlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.

/stats/port <port number>/if
Interface Statistics

This menu option enables you to display the interface statistics of the selected port.

```
Interface statistics for port 1:1:
                     ifHCIn Counters       ifHCOut Counters
Octets:                  51697080313            51721056808
UcastPkts:                  65356399               65385714
BroadcastPkts:                     0                   6516
MulticastPkts:                     0                      0
Discards:                          0                      0
Errors:                            0                  21187
```

Table 5-7 Interface Statistics for Port (/stats/port/if)

Statistics	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher sub- layer, which were not addressed to a multicast or broadcast address at this sub-layer.
ifInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher sub- layer, which were addressed to a broadcast address at this sub-layer.
ifInMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.

Table 5-7 Interface Statistics for Port (/stats/port/if)

Statistics	Description
ifInUnknownProtos	For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces which support protocol multiplexing, the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface which does not support protocol multiplexing, this counter will always be 0.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts.
ifOutMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifOutMulticastPkts.
ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

/stats/port <port number>/ip
Interface Protocol Statistics

This menu option enables you to display the interface statistics of the selected port.

```
GEA IP statistics for port 1:1:
ipInReceives   :         0
ipInHeaderError:         0
ipInDiscards   :         0
```

Table 5-8 Interface Protocol Statistics (/stats/port/ip)

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHeaderErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch).
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

/stats/port <port number>/link
Link Statistics

This menu enables you to display the link statistics of the selected port.

```
Link statistics for port 1:1:
linkStateChange:             1
```

Table 5-9 Link Statistics (/stats/port/link)

Statistics	Description
linkStateChange	The total number of link state changes.

/stats/l2
Layer 2 Statistics

```
[Layer 2 Statistics Menu]
     fdb       - Show FDB stats
     lacp      - Show LACP stats
```

The Layer 2 statistics provided by each menu option are briefly described in Table 5-10, with pointers to detailed information.

Table 5-10 Layer 2 Statistics Menu Options (/stats/l2)

Command Syntax and Usage
fdb [clear] Displays FDB statistics. See page 87 for sample output. Use the following command to clear all FDB statistics: `fdb clear`
lacp *<port number>* **[clear]** Displays Link Aggregation Control Protocol (LACP) statistics. See page 88 for sample output. Use the following command to clear all LACP statistics: `lacp clear`

/stats/l2/fdb [clear]
FDB Statistics

```
FDB statistics:
 current:            83   hiwat:              855
```

This menu option enables you to display statistics regarding the use of the forwarding database, including the number of new entries, finds, and unsuccessful searches. Use the following command to clear all FDB statistics: `fdb clear`

FDB statistics are described in the following table:

Table 5-11 Forwarding Database Statistics (/stats/fdb)

Statistic	Description
`current`	Current number of entries in the Forwarding Database.
`hiwat`	Highest number of entries recorded at any given time in the Forwarding Database.

/stats/l2/lacp <port number> [clear]
LACP Statistics

```
Port 1:1:
 ------------------------------------
 Valid LACPDUs received:          - 870
 Valid Marker PDUs received:      - 0
 Valid Marker Rsp PDUs received: - 0
 Unknown version/TLV type:        - 0
 Illegal subtype received:        - 0
 LACPDUs transmitted:             - 6031
 Marker PDUs transmitted:         - 0
 Marker Rsp PDUs transmitted:     - 0
```

Link Aggregation Control Protocol (LACP) statistics are described in the following table:

Table 5-12 LACP Statistics (/stats/lacp)

Statistic	Description
`Valid LACPDUs received`	Total number of valid LACP data units received.
`Valid Marker PDUs received`	Total number of valid LACP marker data units received.
`Valid Marker Rsp PDUs received`	Total number of valid LACP marker response data units received.
`Unknown version/TLV type`	Total number of LACP data units with an unknown version or type, length, and value (TLV) received.
`Illegal subtype received`	Total number of LACP data units with an illegal subtype received.
`LACPDUs transmitted`	Total number of LACP data units transmitted.
`Marker PDUs transmitted`	Total number of LACP marker data units transmitted.
`Marker Rsp PDUs transmitted`	Total number of LACP marker response data units transmitted.

/stats/l3
Layer 3 Statistics

```
[Layer 3 Statistics Menu]
    ip         - Show IP stats
    arp        - Show ARP stats
    dns        - Show DNS stats
    icmp       - Show ICMP stats
    tcp        - Show TCP stats
    udp        - Show UDP stats
    igmp       - Show IGMP stats
    igmpgrps   - Total number of IGMP groups
    ipmcgrps   - Total number of IPMC groups
    clrigmp    - Clear IGMP stats
    ipclear    - Clear IP stats
    dump       - Dump layer 3 stats
```

The Layer 3 statistics provided by each menu option are briefly described in Table 5-13, with pointers to detailed information.

Table 5-13 Layer 3 Statistics Menu Options (/stats/l3)

Command Syntax and Usage
ip Displays IP statistics. See page 91 for sample output.
arp Displays Address Resolution Protocol (ARP) statistics. See page 93 for sample output.
dns [clear] Displays Domain Name System (DNS) statistics. See page 93 for sample output. Use the following command to clear all DNS statistics: `dns clear`
icmp [clear] Displays ICMP statistics. See page 94 for sample output. Use the following command to clear all ICMP statistics: `icmp clear`
tcp [clear] Displays TCP statistics. See page 96 for sample output. Use the following command to clear all TCP statistics: `tcp clear`
udp [clear] Displays UDP statistics. See page 98 for sample output. Use the following command to clear all UDP statistics: `udp clear`

Table 5-13 Layer 3 Statistics Menu Options (/stats/l3)

Command Syntax and Usage
igmp Displays IGMP statistics. See page 99 for sample output.
igmpgrps Displays the total number of IGMP groups that are registered on the switch.
ipmcgrps Displays the total number of current IP multicast groups that are registered on the switch.
clrigmp Clears IGMP statistics.
ipclear Clears IP statistics. Use this command with caution as it will delete all the IP statistics.
dump Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.

/stats/l3/ip
IP Statistics

```
IP statistics:
ipInReceives:         3115873   ipInHdrErrors:            1
ipInAddrErrors:         35447   ipForwDatagrams:          0
ipInUnknownProtos:     500504   ipInDiscards:             0
ipInDelivers:         2334166   ipOutRequests:      1010542
ipOutDiscards:              4   ipOutNoRoutes:            4
ipReasmReqds:               0   ipReasmOKs:               0
ipReasmFails:               0   ipFragOKs:                0
ipFragFails:                0   ipFragCreates:            0
ipRoutingDiscards:          0   ipDefaultTTL:           255
ipReasmTimeout:             5
```

Table 5-14 IP Statistics (stats/l3/ip)

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipForwDatagrams	The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source- Route option processing was successful.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

Table 5-14 IP Statistics (stats/l3/ip)

Statistics	Description
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams, which meet this *no-route* criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ipReasmReqds	The number of IP fragments received which needed to be reassembled at this entity (the switch).
ipReasmOKs	The number of IP datagrams successfully re- assembled.
ipReasmFails	The number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their Don't Fragment flag was set.
ipFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
ipRoutingDiscards	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
ipDefaultTTL	The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.
ipReasmTimeout	The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch).

/stats/l3/arp
ARP statistics

This menu option enables you to display Address Resolution Protocol statistics.

```
ARP statistics:
arpEntriesCur:              3  arpEntriesHighWater:          4
```

Table 5-15 ARP Statistics (/stats/l3/arp)

Statistics	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.

/stats/l3/dns [clear]
DNS Statistics

This menu option enables you to display Domain Name System statistics.

```
DNS statistics:
dnsInRequests:              0  dnsOutRequests:             0
dnsBadRequests:             0
```

Table 5-16 DNS Statistics (/stats/dns)

Statistics	Description
dnsInRequests	The total number of DNS request packets that have been received.
dnsOutRequests	The total number of DNS response packets that have been transmitted.
dnsBadRequests	The total number of DNS request packets received that were dropped.

/stats/l3/icmp [clear]
ICMP Statistics

```
ICMP statistics:
icmpInMsgs:              245802   icmpInErrors:               1393
icmpInDestUnreachs:          41   icmpInTimeExcds:               0
icmpInParmProbs:              0   icmpInSrcQuenchs:              0
icmpInRedirects:              0   icmpInEchos:                  18
icmpInEchoReps:          244350   icmpInTimestamps:              0
icmpInTimestampReps:          0   icmpInAddrMasks:               0
icmpInAddrMaskReps:           0   icmpOutMsgs:              253810
icmpOutErrors:                0   icmpOutDestUnreachs:          15
icmpOutTimeExcds:             0   icmpOutParmProbs:              0
icmpOutSrcQuenchs:            0   icmpOutRedirects:              0
icmpOutEchos:            253777   icmpOutEchoReps:              18
icmpOutTimestamps:            0   icmpOutTimestampReps:          0
icmpOutAddrMasks:             0   icmpOutAddrMaskReps:           0
```

Table 5-17 ICMP Statistics (/stats/l3/icmp)

Statistics	Description
icmpInMsgs	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by icmpInErrors.
icmpInErrors	The number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so forth).
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.

Table 5-17 ICMP Statistics (/stats/l3/icmp)

Statistics	Description
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs	The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by icmpOutErrors.
icmpOutErrors	The number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

/stats/l3/tcp [clear]
TCP Statistics

```
TCP statistics:
tcpRtoAlgorithm:          4   tcpRtoMin:                0
tcpRtoMax:           240000   tcpMaxConn:             512
tcpActiveOpens:      252214   tcpPassiveOpens:          7
tcpAttemptFails:        528   tcpEstabResets:           4
tcpInSegs:           756401   tcpOutSegs:          756655
tcpRetransSegs:           0   tcpInErrs:                0
tcpCurBuff:               0   tcpCurConn:               3
tcpOutRsts:             417
```

Table 5-18 TCP Statistics (/stats/l3/tcp)

Statistics	Description
tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

Table 5-18 TCP Statistics (/stats/l3/tcp)

Statistics	Description
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP checksums).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.

/stats/l3/udp [clear]
UDP Statistics

```
UDP statistics:
udpInDatagrams:         54   udpOutDatagrams:         43
udpInErrors:             0   udpNoPorts:         1578077
```

Table 5-19 UDP Statistics (/stats/l3/udp)

Statistics	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this entity (the switch).
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

/stats/l3/igmp <VLAN number>
IGMP Statistics

```
IGMP Snoop vlan 2 statistics:
-------------------------------------------------------------------------
rxIgmpValidPkts:                0   rxIgmpInvalidPkts:                0
rxIgmpGenQueries:               0   rxIgmpGrpSpecificQueries:         0
rxIgmpGroupSrcSpecificQueries:  0
rxIgmpLeaves:                   0   rxIgmpReports:                    0
txIgmpReports:                  0   txIgmpGrpSpecificQueries:         0
txIgmpLeaves:                   0   rxIgmpV3CurrentStateRecords:      0
rxIgmpV3SourceListChangeRecords:0   rxIgmpV3FilterChangeRecords:      0
```

This menu option displays statistics about the use of the IGMP Multicast Groups. IGMP statistics are described in the following table:

Table 5-20 IGMP Statistics (/stats/l3/igmp)

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpGrpSpecificQueries	Total number of Membership Query packets received from specific groups
rxIgmpGroupSrcSpecificQueries	Total number of Group Source-Specific Queries (GSSQ) received
rxIgmpLeaves	Total number of Leave requests received
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecificQueries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave messages transmitted
rxIgmpV3CurrentStateRecords	Total number of Current State records received
rxIgmpV3SourceListChangeRecords	Total number of Source List Change records received.
rxIgmpV3FilterChangeRecords	Total number of Filter Change records received.

/stats/mp
Management Processor Statistics

```
[MP-specific Statistics Menu]
      thr     - Show STEM thread stats
      i2c     - Show I2C stats
      pkt     - Show Packet stats
      tcb     - Show All TCP control blocks in use
      ucb     - Show All UDP control blocks in use
      cpu     - Show CPU utilization
```

Table 5-21 Management Processor Statistics Menu Options (/stats/mp)

Command Syntax and Usage
thr Displays STEM thread statistics. This command is used by Technical Support personnel.
i2c Displays I2C statistics. This command is used by Technical Support personnel.
pkt Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 101.
tcb Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see page 102.
ucb Displays all UDP control blocks that are in use. To view a sample output, see page 102.
cpu Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see page 103.

/stats/mp/pkt
MP Packet Statistics

```
Packet counts:
 allocs:        1722684     frees:                      1722684
 mediums:             0     mediums hi-watermark:             4
 jumbos:              0     jumbos hi-watermark:              0
 smalls:              0     smalls hi-watermark:              8
 failures:            0
```

Table 5-22 Packet Statistics (/stats/mp/pkt)

Statistics	Description
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
mediums	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
mediums hi-water-mark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.

/stats/mp/tcb
TCP Statistics

```
All TCP allocated control blocks:
10ad41e8:  0.0.0.0             0 <=> 0.0.0.0            80  listen
10ad5790:  47.81.27.5       1171 <=> 47.80.23.243       23  established
```

Table 5-23 MP Specified TCP Statistics (/stats/mp/tcb)

Statistics	Description
10ad41e8/10ad5790	Memory
0.0.0.0/47.81.27.5	Destination IP address
0/1171	Destination port
0.0.0.0/47.80.23.243	Source IP
80/23	Source port
listen/established	State

/stats/mp/ucb
UCB Statistics

```
All UDP allocated control blocks:
  161:  listen
```

/stats/mp/cpu
CPU Statistics

This menu option enables you to display the CPU utilization statistics.

```
CPU utilization:
cpuUtil1Second:             53%
cpuUtil4Seconds:            54%
cpuUtil64Seconds:           54%
```

Table 5-24 CPU Statistics (stats/mp/cpu)

Statistics	Description
cpuUtil1Second	The utilization of MP CPU over 1 second. It shows the percentage.
cpuUtil4Seconds	The utilization of MP CPU over 4 seconds. It shows the percentage.
cpuUtil64Seconds	The utilization of MP CPU over 64 seconds. It shows the percentage.

/stats/acl
ACL Statistics

```
[ACL Menu]
     acl       - Display ACL stats
     dump      - Display all available ACL stats
     clracl    - Clear ACL stats
```

ACL statistics are described in the following table.

Table 5-25 ACL Statistics Menu Options (/stats/acl)

Command Syntax and Usage
acl *<1-768>* Displays the Access Control List Statistics for a specific ACL. For details, see page 104.
dump Displays all ACL statistics.
clracl Clears all ACL statistics.

/stats/acl/acl *<ACL number>*
ACL Statistics

This option displays ACL statistics.

```
Hits for ACL 1, port 1:1:              26057515
Hits for ACL 2, port 1:1:              26057497
```

/stats/snmp
SNMP Statistics

NOTE – Use the following command to reset the SNMP counter to zero: `snmp clear`

```
SNMP statistics:
snmpInPkts:              150097   snmpInBadVersions:              0
snmpInBadC'tyNames:           0   snmpInBadC'tyUses:              0
snmpInASNParseErrs:           0   snmpEnableAuthTraps:            0
snmpOutPkts:             150097   snmpInBadTypes:                 0
snmpInTooBigs:                0   snmpInNoSuchNames:              0
snmpInBadValues:              0   snmpInReadOnlys:                0
snmpInGenErrs:                0   snmpInTotalReqVars:        798464
snmpInTotalSetVars:        2731   snmpInGetRequests:          17593
snmpInGetNexts:          131389   snmpInSetRequests:            615
snmpInGetResponses:           0   snmpInTraps:                    0
snmpOutTooBigs:               0   snmpOutNoSuchNames:             1
snmpOutBadValues:             0   snmpOutReadOnlys:               0
snmpOutGenErrs:               1   snmpOutGetRequests:             0
snmpOutGetNexts:              0   snmpOutSetRequests:             0
snmpOutGetResponses:     150093   snmpOutTraps:                   4
snmpSilentDrops:              0   snmpProxyDrops:                 0
```

Table 5-26 SNMP Statistics (/stats/snmp)

Statistics	Description
`snmpInPkts`	The total number of Messages delivered to the SNMP entity from the transport service.
`snmpInBadVersions`	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
`snmpInBadC'tyNames`	The total number of SNMP Messages delivered to the SNMP entity which used an SNMP community name not known to the said entity (the switch).
`snmpInBadC'tyUses`	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.

Table 5-26 SNMP Statistics (/stats/snmp)

Statistics	Description
snmpInASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received. **Note:** OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
snmpEnableAuth Traps	An object to enable or disable the authentication traps generated by this entity (the switch).
snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadTypes	The total number of SNMP Messages which failed ASN parsing.
snmpInTooBigs	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is *too big*.
snmpInNoSuchNames	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.
snmpInBadValues	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.
snmpInReadOnlys	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `read-Only'. It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value `read-Only' in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).

Table 5-26 SNMP Statistics (/stats/snmp)

Statistics	Description
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is *too big*.
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is noSuchName.
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is badValue.
snmpOutReadOnlys	Not in use.
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is genErr.
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGet Responses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.

Table 5-26 SNMP Statistics (/stats/snmp)

Statistics	Description
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMPv2 entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner such that no Response-PDU could be returned.

/stats/ntp [clear]
NTP Statistics

BLADE OS uses NTP (Network Timing Protocol) version 3 to synchronize the switch's internal clock with an atomic time calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

Use the following command to clear all NTP statistics: `ntp clear`

```
NTP statistics:
        Primary Server:
                Requests Sent:              17
                Responses Received:         17
                Updates:                    1
        Secondary Server:
                Requests Sent:              0
                Responses Received:         0
                Updates:                    0
        Last update based on response from primary server.
        Last update time: 18:04:16 Tue Jul 17, 2009
        Current system time: 18:55:49 Tue Jul 17, 2009
```

Table 5-27 NTP Statistics Parameters (/stats/ntp)

Field	Description
Primary Server	**Requests Sent:** The total number of NTP requests the switch sent to the primary NTP server to synchronize time. **Responses Received:** The total number of NTP responses received from the primary NTP server. **Updates:** The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
Secondary Server	**Requests Sent:** The total number of NTP requests the switch sent to the secondary NTP server to synchronize time. **Responses Received:** The total number of NTP responses received from the secondary NTP server. **Updates:** The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.

Table 5-27 NTP Statistics Parameters (/stats/ntp)

Field	Description
Last update based on response from primary server	Last update of time on the switch based on either primary or secondary NTP response received.
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The switch system time when the command `/stats/ntp` was issued.

/stats/dump
Statistics Dump

Use the dump command to dump all switch statistics available from the Statistics Menu (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

CHAPTER 6

The Configuration Menu

This chapter discusses how to use the Command Line Interface (CLI) for making, viewing, and saving switch configuration changes. Many of the commands, although not new, display more or different information than in the previous version. Important differences are called out in the text.

/cfg
Configuration Menu

```
[Configuration Menu]
     sys       - System-wide Parameter Menu
     port      - Port Menu
     stack     - Stacking Menu
     qos       - QOS Menu
     acl       - Access Control List Menu
     pmirr     - Port Mirroring Menu
     l2        - Layer 2 Menu
     l3        - Layer 3 Menu
     dump      - Dump current configuration to script file
     ptcfg     - Backup current configuration to FTP/TFTP server
     gtcfg     - Restore current configuration from FTP/TFTP server
     cur       - Display current configuration
```

Each configuration option is briefly described in Table 6-1, with pointers to detailed menu commands.

Table 6-1 Configuration Menu Options (/cfg)

Command Syntax and Usage
sys Displays the System Configuration Menu. To view menu options, see page 115.
port *<port number>* Displays the Port Configuration Menu. To view menu options, see page 146.
stack Displays the Stacking Configuration Menu. To view menu options, see page 150.
qos Displays the Quality of Service Configuration Menu. To view menu options, see page 185.
acl Displays the ACL Configuration Menu. To view menu options, see page 188.
pmirr Displays the Mirroring Configuration Menu. To view menu options, see page 154.
l2 Displays the Layer 2 Configuration Menu. To view menu options, see page 156.
l3 Displays the Layer 3 Configuration Menu. To view menu options, see page 176.

Table 6-1 Configuration Menu Options (/cfg)

Command Syntax and Usage
dump Dumps current configuration to a script file. For details, see page 199.
ptcfg *<host name or IP address of TFTP server> <filename on host>* Backs up current configuration to TFTP server. For details, see page 200.
gtcfg *<host name or IP address of TFTP server> <filename on host>* Restores current configuration from TFTP server. For details, see page 200.
cur Displays current configuration parameters.

Viewing, Applying, and Saving Changes

As you use the configuration menus to set switch parameters, the changes you make do not take effect immediately. All changes are considered "pending" until you explicitly apply them. Also, any changes are lost the next time the switch boots unless the changes are explicitly saved.

NOTE – Some operations can override the settings in the Configuration menu. Therefore, settings you view in the Configuration menu (for example, port status) might differ from run-time information that you view in the Information menu or on the management module. The Information menu displays current run-time information of switch parameters.

While configuration changes are in the pending state, you can do the following:

- View the pending changes
- Apply the pending changes
- Save the changes to flash memory

Viewing Pending Changes

You can view all pending configuration changes by entering **diff** at the menu prompt.

NOTE – The `diff` command is a global command. Therefore, you can enter **diff** at any prompt in the CLI.

Applying Pending Changes

To make your configuration changes active, you must apply them. To apply configuration changes, enter **apply** at any prompt in the CLI.

```
# apply
```

NOTE – The apply command is a global command. Therefore, you can enter **apply** at any prompt in the administrative interface.

Saving the Configuration

In addition to applying the configuration changes, you can save them to flash memory on the G8000.

NOTE – If you do not save the changes, they will be lost the next time the system is rebooted.

To save the new configuration, enter the following command at any CLI prompt:

```
# save
```

When you save configuration changes, the changes are saved to the *active* configuration block. The configuration being replaced by the save is first copied to the *backup* configuration block. If you do not want the previous configuration block copied to the backup configuration block, enter the following instead:

```
# save n
```

You can decide which configuration you want to run the next time you reset the switch. Your options include:

- The active configuration block
- The backup configuration block
- Factory default configuration

You can view all pending configuration changes that have been applied but not saved to flash memory using the diff flash command. It is a global command that can be executed from any menu.

For instructions on selecting the configuration to run at the next system reset, see "Selecting a Configuration Block" on page 210.

/cfg/sys
System Configuration

```
[System Menu]
     syslog   - Syslog Menu
     sshd     - SSH Server Menu
     radius   - RADIUS Authentication Menu
     tacacs+  - TACACS+ Authentication Menu
     ntp      - NTP Server Menu
     ssnmp    - System SNMP Menu
     access   - System Access Menu
     date     - Set system date
     time     - Set system time
     timezone - Set system timezone (daylight savings)
     dlight   - Set system daylight savings
     idle     - Set timeout for idle CLI sessions
     notice   - Set login notice
     bannr    - Set login banner
     hprompt  - Enable/disable display hostname (sysName) in CLI prompt
     dhcp     - Enable/disable use of DHCP on Mgmt interface
     rstctrl  - Enable/disable System reset on panic
     cur      - Display current system-wide parameters
```

This menu provides configuration of switch management parameters such as user and administrator privilege mode passwords, Web-based management settings, and management access lists.

Table 6-2 System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
syslog Displays the Syslog Menu. To view menu options, see page 118.
sshd Displays the SSH Server Menu. To view menu options, see page 119.
radius Displays the RADIUS Authentication Menu. To view menu options, see page 121.
tacacs+ Displays the TACACS+ Authentication Menu. To view menu options, see page 123.
ntp Displays the Network Time Protocol (NTP) Server Menu. To view menu options, see page 126.
ssnmp Displays the System SNMP Menu. To view menu options, see page 127.

Table 6-2 System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
access Displays the System Access Menu. To view menu options, see page 140.
date Prompts the user for the system date. The date reverts to its default value when the switch is reset.
time Configures the system time using a 24-hour clock format. The time reverts to its default value when the switch is reset.
timezone Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.
dlight enable|disable Disables or enables daylight savings time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. The default value is **disabled**.
idle *<idle timeout in minutes>* Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 10 minutes.
notice *<max 1024 char multi-line login notice> <'-' to end>* Displays login notice immediately before the "Enter password:" prompt. This notice can contain up to 1024 characters and new lines.
bannr *<string, maximum 80 characters>* Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the `/info/sys` command.
hprompt disable|enable Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).
dhcp disable|enable Enables or disables Dynamic Host Control Protocol for setting the IP address on the management interface. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default value is `enabled`.

Table 6-2 System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
rstctrl disable|enable Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information. The default value is `enabled`.
cur Displays the current system parameters.

/cfg/sys/syslog
System Host Log Configuration

```
[Syslog Menu]
     host      - Set IP address of first syslog host
     host2     - Set IP address of second syslog host
     sever     - Set the severity of first syslog host
     sever2    - Set the severity of second syslog host
     facil     - Set facility of first syslog host
     facil2    - Set facility of second syslog host
     console   - Enable/disable console output of syslog messages
     log       - Enable/disable syslogging of features
     cur       - Display current syslog settings
```

Table 6-3 Host Log Menu Options (/cfg/sys/syslog)

Command Syntax and Usage
host *<new syslog host IP address (such as, 192.4.17.223)>* Sets the IP address of the first syslog host.
host2 *<new syslog host IP address (such as, 192.4.17.223)>* Sets the IP address of the second syslog host.
sever *<syslog host local severity (0–7)>* This option sets the severity level of the first syslog host displayed. The default is 7, which means log all severity levels.
sever2 *<syslog host local severity (0–7)>* This option sets the severity level of the second syslog host displayed. The default is 7, which means, log all severity levels.
facil *<syslog host local facility (0-7)>* This option sets the facility level of the first syslog host displayed. The default is 0.
facil2 *<syslog host local facility (0-7)>* This option sets the facility level of the second syslog host displayed. The default is 0.
console disable|enable Enables or disables delivering syslog messages to the console. When necessary, disabling `console` ensures the switch is not affected by syslog messages. It is enabled by default.
log *<feature|all> <enable|disable>* Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as vlans, stg, or servers), or enable/disable syslog on all available features.
cur Displays the current syslog settings.

/cfg/sys/sshd
SSH Server Configuration

```
[SSHD Menu]
     intrval  - Set Interval for generating the RSA server key
     scpadm   - Set SCP-only admin password
     hkeygen  - Generate the RSA host key
     skeygen  - Generate the RSA server key
     sshport  - Set SSH server port number
     ena      - Enable the SCP apply and save
     dis      - Disable the SCP apply and save
     on       - Turn SSH server ON
     off      - Turn SSH server OFF
     cur      - Display current SSH server configuration
```

This menu enables Secure Shell access from any SSH client. SSH scripts can be viewed by using the `/cfg/dump` command (see page 199).

Table 6-4 System Configuration Menu Options (/cfg/sys/sshd)

Command Syntax and Usage
intrval *<0 - 24>* Set the interval for auto-generation of the RSA server key.
scpadm Set the administration password for SCP access.
hkeygen Generate the RSA host key.
skeygen Generate the RSA server key.
sshport *<TCP port number>* Sets the SSH server port number.
ena Enables the SCP apply and save.
dis Disables the SCP apply and save.
on Enables the SSH server.

Table 6-4 System Configuration Menu Options (/cfg/sys/sshd)

Command Syntax and Usage
off Disables the SSH server.
cur Displays the current SSH server configuration.

/cfg/sys/radius
RADIUS Server Configuration

```
[RADIUS Server Menu]
 prisrv  - Set primary RADIUS server address
 secsrv  - Set secondary RADIUS server address
 secret  - Set RADIUS secret
 secret2 - Set secondary RADIUS server secret
 port    - Set RADIUS port
 retries - Set RADIUS server retries
 timeout - Set RADIUS server timeout
 bckdoor  - Enable/disable RADIUS backdoor for telnet/ssh/http/https
 secbd    - Enable/disable RADIUS secure backdoor for telnet/ssh/
            http/https
 on      - Turn RADIUS authentication ON
 off     - Turn RADIUS authentication OFF
 cur     - Display current RADIUS configuration
```

Table 6-5 System Configuration Menu Options (/cfg/sys/radius)

Command Syntax and Usage
prisrv *<IP address>* Sets the primary RADIUS server address.
secsrv *<IP address>* Sets the secondary RADIUS server address.
secret *<1-32 character secret>* This is the shared secret between the switch and the RADIUS server(s).
secret2 *<1-32 character secret>* This is the secondary shared secret between the switch and the RADIUS server(s).
port *<RADIUS port configure, default 1645>* Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.
retries *<RADIUS server retries (1-3)>* Sets the number of failed authentication requests before switching to a different RADIUS server. The default is 3 requests.
timeout *<RADIUS server timeout seconds (1-10)>* Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is 3 seconds.
bckdoor disable|enable Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is `disabled`. To obtain the RADIUS backdoor password, contact your Service and Support line.

Table 6-5 System Configuration Menu Options (/cfg/sys/radius)

Command Syntax and Usage
secbd disable|enable Enables or disables RADIUS secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the RADIUS servers are not responding. This feature is recommended to permit access to the switch when the RADIUS servers become unresponsive. If no back door is enabled, the only way to gain access when RADIUS servers are unresponsive is to use the back door via the console port. The default is `disabled`.
on Enables the RADIUS server.
off Disables the RADIUS server.
cur Displays the current RADIUS server parameters.

/cfg/sys/tacacs+
TACACS+ Server Configuration

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is an encryption protocol, and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. (Both TACACS and TACACS+ are described in RFC 1492.)

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports de-coupled authentication, authorization, and accounting.

```
[TACACS+ Server Menu]
     prisrv   - Set IP address of primary TACACS+ server
     secsrv   - Set IP address of secondary TACACS+ server
     secret   - Set secret for primary TACACS+ server
     secret2  - Set secret for secondary TACACS+ server
     port     - Set TACACS+ port number
     retries  - Set number of TACACS+ server retries
     timeout  - Set timeout value of TACACS+ server retries
     usermap  - Set user privilege mappings
     bckdoor  - Enable/disable TACACS+ backdoor for telnet/ssh/http/
                https
     secbd    - Enable/disable TACACS+ secure backdoor
     cmap     - Enable/disable TACACS+ new privilege level mapping
     on       - Enable TACACS+ authentication
     off      - Disable TACACS+ authentication
     cur      - Display current TACACS+ settings
```

Table 6-6 TACACS+ Server Menu Options (/cfg/sys/tacacs)

Command Syntax and Usage
prisrv *<IP address>* Defines the primary TACACS+ server address.
secsrv *<IP address>* Defines the secondary TACACS+ server address.
secret *<1-32 character secret>* This is the shared secret between the switch and the TACACS+ server(s).
secret2 *<1-32 character secret>* This is the secondary shared secret between the switch and the TACACS+ server(s).
port *<TACACS port configure, default 49>* Enter the number of the TCP port to be configured, between 1 - 65000. The default is 49.
retries <*TACACS server retries, 1-3>* Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests.
timeout *<TACACS server timeout seconds, 4-15>* Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is 5 seconds.
usermap *<0-15>* **user|oper|admin|none** Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level.
bckdoor disable|enable Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS. Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding. The default is `disabled`. To obtain the TACACS+ backdoor password for your switch, contact your Service and Support line.
secbd enable|disable Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding. This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port. The default is `disabled`.

Table 6-6 TACACS+ Server Menu Options (/cfg/sys/tacacs)

Command Syntax and Usage
cmap enable|disable Enables or disables TACACS+ privilege-level mapping. The default value is `disabled`.
on Enables the TACACS+ server. This is the default setting.
off Disables the TACACS+ server.
cur Displays current TACACS+ configuration parameters.

/cfg/sys/ntp
NTP Server Configuration

```
[NTP Server Menu]
      prisrv  - Set primary NTP server address
      secsrv  - Set secondary NTP server address
      intrval - Set NTP server resync interval
      on      - Turn NTP service ON
      off     - Turn NTP service OFF
      cur     - Display current NTP configuration
```

This menu enables you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

Table 6-7 NTP Configuration Menu Options (/cfg/sys/ntp)

Command Syntax and Usage
prisrv *<NTP Server IP address>* Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock.
secsrv *<NTP Server IP address>* Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock.
intrval *<1-44640>* Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server.
on Enables the NTP synchronization service.
off Disables the NTP synchronization service.
cur Displays the current NTP service settings.

cfg/sys/ssnmp
System SNMP Configuration

```
[System SNMP Menu]
     snmpv3    - SNMPv3 Menu
     name      - Set SNMP "sysName"
     locn      - Set SNMP "sysLocation"
     cont      - Set SNMP "sysContact"
     rcomm     - Set SNMP read community string
     wcomm     - Set SNMP write community string
     trsrc     - Set SNMP trap source interface
     timeout   - Set timeout for the SNMP state machine
     auth      - Enable/disable SNMP "sysAuthenTrap"
     linkt     - Enable/disable SNMP link up/down trap
     cur       - Display current SNMP configuration
```

BLADE OS supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

SNMP parameters that can be modified include:

- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string
- Trap community strings

Table 6-8 System SNMP Menu Options (/cfg/sys/ssnmp)

Command Syntax and Usage
snmpv3 Displays SNMPv3 menu. To view menu options, see page 129.
name *<new string, maximum 64 characters>* Configures the name for the system. The name can have a maximum of 64 characters.
locn *<new string, maximum 64 characters>* Configures the name of the system location. The location can have a maximum of 64 characters.
cont *<new string, maximum 64 characters>* Configures the name of the system contact. The contact can have a maximum of 64 characters.
rcomm *<new SNMP read community string, maximum 32 characters>* Configures the SNMP read community string. The read community string controls SNMP "get" access to the switch. It can have a maximum of 32 characters. The default read community string is *public*.
wcomm *<new SNMP write community string, maximum 32 characters>* Configures the SNMP write community string. The write community string controls SNMP "set" and "get" access to the switch. It can have a maximum of 32 characters. The default write community string is *private*.
trsrc *<1-128>* Configures the source interface for SNMP traps.
timeout *<1-30>* Set the timeout value for the SNMP state machine, in minutes.
auth disable|enable Enables or disables the use of the system authentication trap facility. The default setting is disabled.
linkt *<port>* [**disable|enable**] Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled.
cur Displays the current SNMP configuration.

/cfg/sys/ssnmp/snmpv3
SNMPv3 Configuration

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC2271 to RFC2276.

```
[SNMPv3 Menu]
     usm       - usmUser Table menu
     view      - vacmViewTreeFamily Table menu
     access    - vacmAccess Table menu
     group     - vacmSecurityToGroup Table menu
     comm      - community Table menu
     taddr     - targetAddr Table menu
     tparam    - targetParams Table menu
     notify    - notify Table menu
     v1v2      - Enable/disable V1/V2 access
     cur       - Display current SNMPv3 configuration
```

Table 6-9 SNMPv3 Configuration Menu Options (/cfg/sys/ssnmp/snmpv3)

Command Syntax and Usage
usm *<usmUser number [1-16]>* This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. To view menu options, see page 131.
view *<vacmViewTreeFamily number [1-128]>* This command allows you to create different MIB views. To view menu options, see page 132.
access *<vacmAccess number [1-32]>* This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. To view menu options, see page 133.
group *<vacmSecurityToGroup number [1-16]>* A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. To view menu options, see page 135.

Table 6-9 SNMPv3 Configuration Menu Options (/cfg/sys/ssnmp/snmpv3)

comm *<snmpCommunity number [1-16]>*

The community table contains objects for mapping community strings and version-independent SNMP message parameters. To view menu options, see page 136.

taddr *<snmpTargetAddr number [1-16]>*

This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. To view menu options, see page 137.

tparam *<target params index [1-16]>*

This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. To view menu options, see page 138.

notify *<notify index [1-16]>*

A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. To view menu options, see page 139.

v1v2 disable|**enable**

This command allows you to enable or disable the access to SNMP version 1 and version 2. This command is enabled by default.

cur

Displays the current SNMPv3 configuration.

/cfg/sys/ssnmp/snmpv3/usm
User Security Model Configuration

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

This menu helps you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

```
[SNMPv3 usmUser 1  Menu]
     name      - Set USM user name
     auth      - Set authentication protocol
     authpw    - Set authentication password
     priv      - Set privacy protocol
     privpw    - Set privacy password
     del       - Delete usmUser entry
     cur       - Display current usmUser configuration
```

Table 6-10 User Security Model Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/usm)

Command Syntax and Usage
name *<32 character name>* This command allows you to configure a string up to 32 characters long that represents the name of the user. This is the login name that you need in order to access the switch.
auth md5|**sha**|**none** This command allows you to configure the authentication protocol between HMAC-MD5-96 or HMAC-SHA-96. The default algorithm is `none`.
authpw If you selected an authentication algorithm using the above command, you need to provide a password, otherwise you will get an error message during validation. This command allows you to create or change your password for authentication.
priv des|**none** This command allows you to configure the type of privacy protocol on your switch. The privacy protocol protects messages from disclosure. The options are `des` (CBC-DES Symmetric Encryption Protocol) or `none`. If you specify `des` as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select `none` as the authentication protocol, you will get an error message.
privpw This command allows you to create or change the privacy password.

Table 6-10 User Security Model Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/usm)

Command Syntax and Usage
del Deletes the USM user entries.
cur Displays the USM user entries.

cfg/sys/ssnmp/snmpv3/view
SNMPv3 View Configuration

```
[SNMPv3 vacmViewTreeFamily 1  Menu]
    name    - Set view name
    tree    - Set MIB subtree(OID) which defines a family of view subtrees
    mask    - Set view mask
    type    - Set view type
    del     - Delete vacmViewTreeFamily entry
    cur     - Display current vacmViewTreeFamily configuration
```

Table 6-11 SNMPv3 View Menu Options (/cfg/sys/ssnmp/snmpv3/view)

Command Syntax and Usage
name *<32 character name>* This command defines the name for a family of view subtrees up to a maximum of 32 characters.
tree *<object identifier, such as,. 1.3.6.1.2.1.1.1.0, max 32 characters>* This command defines MIB tree, a string of maximum 32 characters, which when combined with the corresponding mask defines a family of view subtrees.
mask *<bitmask, max size 32 characters>* This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees.
type included|excluded This command indicates whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is included in or excluded from the MIB view.
del Deletes the `vacmViewTreeFamily` group entry.
cur Displays the current `vacmViewTreeFamily` configuration.

/cfg/sys/ssnmp/snmpv3/access

View-based Access Control Model Configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

```
[SNMPv3 vacmAccess 1  Menu]
     name      - Set group name
     prefix    - Set content prefix
     model     - Set security model
     level     - Set minimum level of security
     match     - Set prefix only or exact match
     rview     - Set read view index
     wview     - Set write view index
     nview     - Set notify view index
     del       - Delete vacmAccess entry
     cur       - Display current vacmAccess configuration
```

Table 6-12 View-based Access Control Model Menu Options (/cfg/sys/ssnmp/snmpv3/access)

Command Syntax and Usage
name *<32 character name>* Defines the name of the group.
prefix *<32 character name>* Defines the name of the context. An SNMP context is a collection of management information that an SNMP entity can access. An SNMP entity has access to many contexts. For more information on naming the management information, see RFC2571, the SNMP Architecture document. The view-based Access Control Model defines a table that lists the locally available contexts by contextName.
model usm|snmpv1|snmpv2 Allows you to select the security model to be used.
level noAuthNoPriv|authNoPriv|authPriv Defines the minimum level of security required to gain access rights. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol.
match exact|prefix If the value is set to `exact`, then all the rows whose contextName exactly matches the prefix are selected. If the value is set to `prefix` then the all the rows where the starting octets of the contextName exactly match the prefix are selected.

Table 6-12 View-based Access Control Model Menu Options (/cfg/sys/ssnmp/snmpv3/access)

Command Syntax and Usage
rview *<32 character view name>* This is a 32 character long read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.
wview *<32 character view name>* This is a 32 character long write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.
nview *<32 character view name>* This is a 32 character long notify view name that allows you notify access to the MIB view.
del Deletes the View-based Access Control entry.
cur Displays the View-based Access Control configuration.

/cfg/sys/ssnmp/snmpv3/group
SNMPv3 Group Configuration

```
[SNMPv3 vacmSecurityToGroup 1  Menu]
     model     - Set security model
     uname     - Set USM user name
     gname     - Set group gname
     del       - Delete vacmSecurityToGroup entry
     cur       - Display current vacmSecurityToGroup configuration
```

Table 6-13 SNMPv3 Group Menu Options (/cfg/sys/ssnmp/snmpv3/group)

Command Syntax and Usage
model usm|**snmpv1**|**snmpv2** Defines the security model.
uname *<32 character name>* Sets the user name as defined in `/cfg/sys/ssnmp/snmpv3/usm/name` on page 131.
gname *<32 character name>* The name for the access group as defined in `/cfg/sys/ssnmp/snmpv3/access/name` on page 133.
del Deletes the `vacmSecurityToGroup` entry.
cur Displays the current `vacmSecurityToGroup` configuration.

/cfg/sys/ssnmp/snmpv3/comm
SNMPv3 Community Table Configuration

This command is used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

```
[SNMPv3 snmpCommunityTable 1  Menu]
     index     - Set community index
     name      - Set community string
     uname     - Set USM user name
     tag       - Set community tag
     del       - Delete communityTable entry
     cur       - Display current communityTable configuration
```

Table 6-14 SNMPv3 Community Table Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/comm)

Command Syntax and Usage
index *<32 character name>* Allows you to configure the unique index value of a row in this table consisting of 32 characters maximum.
name *<32 character name>* Defines the user name as defined in `/cfg/sys/ssnmp/snmpv3/usm/name` on page 131.
uname *<32 character name>* Defines a readable 32 character long string that represents the corresponding value of an SNMP community name in a security model.
tag *<list of tag string, max 255 characters>* Allows you to configure a tag of up to 255 characters maximum. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap.
del Deletes the community table entry.
cur Displays the community table configuration.

/cfg/sys/ssnmp/snmpv3/taddr
SNMPv3 Target Address Table Configuration

This command is used to configure the target transport entry. The configured entry is stored in the target address table list in the SNMP engine. This table of transport addresses is used in the generation of SNMP messages.

```
[SNMPv3 snmpTargetAddrTable 1  Menu]
     name     - Set target address name
     addr     - Set target transport address IP
     port     - Set target transport address port
     taglist  - Set tag list
     pname    - Set targetParams name
     del      - Delete targetAddrTable entry
     cur      - Display current targetAddrTable configuration
```

Table 6-15 Target Address Table Menu Options (/cfg/sys/ssnmp/snmpv3/taddr)

Command Syntax and Usage
name *<32 character name>* Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry.
addr *<transport address ip>* Allows you to configure a transport address IP that can be used in the generation of SNMP traps.
port *<transport address port>* Allows you to configure a transport address port that can be used in the generation of SNMP traps.
taglist *<list of tag string, max 255 characters>* Allows you to configure a list of tags that are used to select target addresses for a particular operation.
pname *<32 character name>* Defines the name as defined in `/cfg/sys/ssnmp/snmpv3/tparam/name` on page 138.
del Deletes the Target Address Table entry.
cur Displays the current Target Address Table configuration.

/cfg/sys/ssnmp/snmpv3/tparam

SNMPv3 Target Parameters Table Configuration

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (`noAuthnoPriv`, `authNoPriv`, or `authPriv`).

```
[SNMPv3 snmpTargetParamsTable 1  Menu]
     name      - Set target params name
     mpmodel   - Set message processing model
     model     - Set security model
     uname     - Set USM user name
     level     - Set minimum level of security
     del       - Delete targetParamsTable entry
     cur       - Display current targetParamsTable configuration
```

Table 6-16 Target Parameters Table Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/tparam)

Command Syntax and Usage
name *<32 character name>* Allows you to configure the locally arbitrary, but unique identifier that is associated with this entry.
mpmodel snmpv1|snmpv2c|snmpv3 Allows you to configure the message processing model that is used to generate SNMP messages.
model usm|snmpv1|snmpv2 Allows you to select the security model to be used when generating the SNMP messages.
uname *<32 character name>* Defines the name that identifies the user in the USM table (page 131) on whose behalf the SNMP messages are generated using this entry.
level noAuthNoPriv|authNoPriv|authPriv Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol.
del Deletes the `targetParamsTable` entry.
cur Displays the current `targetParamsTable` configuration.

/cfg/sys/ssnmp/snmpv3/notify

SNMPv3 Notify Table Configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

```
[SNMPv3 snmpNotifyTable 1  Menu]
     name      - Set notify name
     tag       - Set notify tag
     del       - Delete notifyTable entry
     cur       - Display current notifyTable configuration
```

Table 6-17 Notify Table Menu Options (/cfg/sys/ssnmp/snmpv3/notify)

Command Syntax and Usage
name *<32 character name>* Defines a locally arbitrary but unique identifier associated with this SNMP notify entry.
tag *<list of tag string, max 255 characters>* Allows you to configure a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the `snmpTargetAddrTable`, that matches the value of this tag, is selected.
del Deletes the notify table entry.
cur Displays the current notify table configuration.

cfg/sys/access
System Access Configuration

```
[System Access Menu]
     mgmt      - Management Network Definition Menu
     user      - User Access Control Menu (passwords)
     https     - HTTPS Web Access Menu
     snmp      - Set SNMP access control
     tnport    - Set Telnet server port number
     tport     - Set the TFTP Port for the system
     wport     - Set HTTP (Web) server port number
     http      - Enable/disable HTTP (Web) access
     tnet      - Enable/disable Telnet access
     tsbbi     - Enable/disable Telnet/SSH configuration from BBI
     userbbi   - Enable/disable user configuration from BBI
     cur       - Display current system access configuration
```

Table 6-18 System Access Menu Options (/cfg/sys/access)

Command Syntax and Usage
mgmt Displays the Management Configuration Menu. To view menu options, see page 142.
user Displays the User Access Control Menu. To view menu options, see page 143.
https Displays the HTTPS Menu. To view menu options, see page 145.
snmp disable|read-only|read-write Disables or provides read-only/write-read SNMP access.
tnport *<TCP port number>* Sets an optional telnet server port number for cases where the server listens for telnet sessions on a non-standard port.
tport *<TFTP port number (1-65535)>* Sets the TFTP port for the switch. The default is port 69.
wport *<TCP port number (1-65535)>* Sets the switch port used for serving switch Web content. The default is HTTP port 80. If Global Server Load Balancing is to be used, set this to a different port (such as 8080).
http disable|enable Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default.
tnet enable|disable Enables or disables Telnet access. This command is enabled by default.

Table 6-18 System Access Menu Options (/cfg/sys/access)

Command Syntax and Usage
tsbbi enable|disable Enables or disables Telnet/SSH configuration access through the Browser-Based Interface (BBI).
userbbi enable|disable Enables or disables user configuration access through the Browser-Based Interface (BBI).
cur Displays the current system access parameters.

/cfg/sys/access/mgmt
Management Networks Configuration

```
[Management Networks Menu]
     add      - Add mgmt network definition
     rem      - Remove mgmt network definition
     cur      - Display current mgmt network definitions
     clear    - Clear current mgmt network definitions
```

This menu is used to define IP address ranges which are allowed to access the switch for management purposes.

Table 6-19 Management Network Menu Options (/cfg/sys/access/mgmt)

Command Syntax and Usage
add *<mgmt network address> <mgmt network mask>* Adds a defined network through which switch access is allowed through Telnet, SNMP, SSH, or the BLADE OS browser-based interface (BBI). A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation. **Note**: If you configure the management network without including the switch interfaces, it will cause the Firewall Load Balancing health checks to fail and will create a "Network Down" state on the network.
rem *<mgmt network address> <mgmt network mask>* Removes a defined network, which consists of a management network address and a management network mask address.
cur Displays the current configuration.
clear Removes all defined management networks.

/cfg/sys/access/user
User Access Control Configuration

```
[User Access Control Menu]
     uid      - User ID Menu
     eject    - Eject user
     usrpw    - Set user password (user)
     opw      - Set operator password (oper)
     admpw    - Set administrator password (admin)
     strongpw - Strong password menu
     cur      - Display current user status
```

NOTE – User passwords can be a maximum of 128 characters.

Table 6-20 User Access Control Menu Options (/cfg/sys/access/user)

Command Syntax and Usage
uid *<User ID (1-10)>* Displays the User ID Menu. To view menu options, see page 144.
eject user|oper|admin|<*user name***>** Ejects the specified user from the switch.
usrpw *<1-128 characters>* Sets the user (`user`) password. The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes. The user password can have a maximum of 128 characters.
opw *<1-128 characters>* Sets the operator (`oper`) password. The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports or the entire switch. The operator password can have a maximum of 128 characters.
admpw *<1-128 characters>* Sets the administrator (`admin`) password. The super user administrator has complete access to all menus, information, and configuration commands on the G8000, including the ability to change both the user and administrator passwords. Access includes "`oper`" functions.
cur Displays the current user status.

/cfg/sys/access/user/uid <1-10>
System User ID Configuration

```
[User ID 1  Menu]
     cos      - Set class of service
     name     - Set user name
     pswd     - Set user password
     ena      - Enable user ID
     dis      - Disable user ID
     del      - Delete user ID
     cur      - Display current user configuration
```

Table 6-21 User ID Configuration Menu Options (/cfg/sys/access/user/uid)

Command Syntax and Usage
cos *<user | oper | admin>* Sets the Class-of-Service to define the user's authority level. BLADE OS defines these levels as: User, Operator, and Administrator, with User being the most restricted level.
name *<1-8 characters>* Defines the user name of maximum eight characters.
pswd *<1-128 characters>* Sets the user password of up to 128 characters.
ena Enables the user ID.
dis Disables the user ID.
del Deletes the user ID.
cur Displays the current user ID configuration.

/cfg/sys/access/https
HTTPS Access Configuration

```
[https Menu]
     access   - Enable/Disable HTTPS Web access
     port     - HTTPS WebServer port number
     generate - Generate self-signed HTTPS server certificate
     certSave - save HTTPS certificate
     cur      - Display current SSL Web Access configuration
```

Table 6-22 HTTPS Access Configuration Menu Options (/cfg/sys/access/https)

Command Syntax and Usage
access ena|dis Enables or disables BBI access (Web access) using HTTPS.
port *<TCP port number>* Defines the HTTPS Web server port number.
generate Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example: ■ Country Name (2 letter code) [ ]: CA ■ State or Province Name (full name) []: Ontario ■ Locality Name (for example, city) []: Ottawa ■ Organization Name (for example, company) []: Blade ■ Organizational Unit Name (for example, section) []: Alteon ■ Common Name (for example, user's name) []: Mr Smith ■ Email (for example, email address) []: info@bladenetwork.net You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent.
certSave Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.
cur Displays the current SSL Web Access configuration.

/cfg/port <port number>
Port Configuration

```
[Port 1:1 Menu]
     gig      - Gig Phy Menu
     aclqos   - Acl/Qos Configuration Menu
     8021ppri - Set default 802.1p priority
     pvid     - Set default port VLAN id
     name     - Set port name
     bpdugrd  - Enable/disable BPDU Guard
     dscpmrk  - Enable/disable DSCP remarking for port
     tag      - Enable/disable VLAN tagging for port
     tagpvid  - Enable/disable tagging on pvid
     ena      - Enable port
     dis      - Disable port
     cur      - Display current port configuration
```

Use the Port Configuration menu to configure settings for individual switch ports.

Table 6-23 Port Configuration Menu (/cfg/port)

Command Syntax and Usage
gig If a port is configured to support Gigabit Ethernet, this option displays the Gigabit Ethernet Physical Link Menu. To view menu options, see page 148.
aclqos Displays the ACL Quality of Service Menu. To view menu options, see page 149.
8021ppri *<0-7>* Configures the port's 802.1p priority level.
pvid *<VLAN number, 1-4095>* Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1 for non-management ports.
name *<64 character string>* | **none** Sets a name for the port. The assigned port name appears next to the port number on some information and statistics screens. The default is set to `none`.
bpdugrd enable|disable Enables or disables BPDU Guard on the port. If Spanning Tree BPDUs are received on the port, BPDU Guard disables the port.
dscpmark Enables or disables DSCP re-marking on a port.

Table 6-23 Port Configuration Menu (/cfg/port)

Command Syntax and Usage
tag disable|enable Disables or enables VLAN tagging for this port. The default value is **disabled**.
tagpvid disable|enable Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default value is `disabled` for internal and external ports, and `enabled` for the management ports.
ena Enables the port.
dis Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to "Temporarily Disabling a Port" on page 149.)
cur Displays current port parameters.

/cfg/port <port number> gig
Port Link Configuration

```
[Gigabit Link Menu]
      speed   - Set link speed
      mode    - Set full or half duplex mode
      fctl    - Set flow control
      auto    - Set auto negotiation
      cur     - Display current gig link configuration
```

Use these menu options to set port parameters for the port link.

Link menu options are described in Table 6-24 and appear on the `gig` port configuration menu for the switch. Use this menu to set port parameters such as speed, flow control, and negotiation mode for the port link.

Table 6-24 Port Link Configuration Menu Options (/cfg/port/gig)

Command Syntax and Usage
speed 10|100|1000|any Sets the link speed. Some options are not valid on all ports. The choices include: ■ 10 Mbps ■ 100 Mbps ■ 1000 Mbps ■ "Auto," for auto negotiation
mode full|half|any Sets the operating mode. The choices include: ■ "Any," for auto negotiation (default) ■ Full-duplex ■ Half-duplex
fctl rx|tx|both|none Sets the flow control. The choices include: ■ Receive flow control ■ Transmit flow control ■ Both receive and transmit flow control (default) ■ No flow control
auto on|off Enables or disables auto negotiation for the port.
cur Displays current port parameters.

Temporarily Disabling a Port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
Main# /oper/port <port number>/dis
```

Because this configuration sets a temporary state for the port, you do not need to use `apply` or `save`. The port state will revert to its original configuration when the switch is reset. See the "Operations Menu" on page 201 for other operations-level commands.

/cfg/port <port number> aclqos
Port ACL Configuration

```
[Port 1:2 ACL Menu]
     add      - Add ACL or ACL group to this port
     rem      - Remove ACL or ACL group from this port
     cur      - Display current ACLs for this port
```

Table 6-25 Port ACL Menu Options (/cfg/port/aclqos)

Command Syntax and Usage
add acl|grp *<ACL number or Group number, 1-768>* Adds the specified ACL or ACL Group to the port. You can add multiple ACL Groups to a port, but the total number of precedence levels allowed is eight.
rem *<ACL number, 1-768>* Removes the specified ACL or ACL Group from the port.
cur Displays current ACL QoS parameters.

/cfg/stack
Stacking Configuration

```
[Stacking Menu]
     swnum    - Switch Number Menu
     mif      - Master Switch Interface Menu
     bif      - Backup Switch Interface Menu
     name     - Set stack name
     backup   - Set backup switch number
     cur      - Display current stacking configuration
```

A *stack* is a group of switches that work together as a unified system. The network views a stack of switches as a single entity, identified by a single network IP address. The Stacking Configuration menu is used to configure a stack, and to define the Master and Backup interface that represents the stack on the network.

Table 6-26 Stacking Menu Options (/cfg/stack)

Command Syntax and Usage
swnum Displays the Stacking Switch menu. To view menu options, see page 151.
mif Displays the Master Switch Interface menu. To view menu options, see page 152.
bif Displays the Backup Switch Interface menu. To view menu options, see page 153.
name *<1-32 characters>* Configures a name for the stack.
backup *<csnum (1-6)>* Defines the backup switch, based on its configured switch number (csnum).
cur Displays current stacking parameters.

/cfg/stack/swnum <switch number>
Stacking Switch Configuration

```
[Switch 1 Menu]
     bind      - Bind UUID with switch in stack
     mac       - Set UUID with MAC addr
     del       - Delete switch
     cur       - Display current Switch configuration
```

Table 6-27 Stacking Switch menu options (/cfg/stack/swnum)

Command Syntax and Usage
bind *<asnum>* Binds the selected switch to the stack, based on its assigned switch number (asnum).
mac *<MAC address>* Binds the selected switch to the stack, based on its MAC address.
del Deletes the selected switch from the stack.
cur Displays the current stacking switch parameters.

/cfg/stack/mif
Master Switch Interface Configuration

```
[Master Switch Interface Menu]
     addr      - Set IP address
     mask      - Set subnet mask
     vlan      - Set VLAN number
     gw        - Set Default Gateway address
     del       - Delete Master IP interface & Default Gateway
     cur       - Display current interface configuration
```

Table 6-28 Master Switch Interface menu options (/cfg/stack/mif)

Command Syntax and Usage
addr *<IP address>* Configures the IP address for the Master Switch Interface, using dotted decimal notation.
mask *<subnet mask>* Configures the IP subnet address mask for the interface, using dotted decimal notation.
vlan *<1-4095>* Configures the VLAN number for this interface.
gw *<IP address>* Configures the default gateway for the Master Switch Interface.
del Deletes the Master Switch Interface.
cur Displays the current Master Switch Interface parameters.

/cfg/stack/bif
Backup Switch Interface Configuration

```
[Backup Switch Interface Menu]
     addr      - Set IP address
     mask      - Set subnet mask
     vlan      - Set VLAN number
     gw        - Set Default Gateway address
     del       - Delete Backup IP interface & Default Gateway
     cur       - Display current interface configuration
```

Table 6-29 Backup Switch Interface menu options (/cfg/stack/bif)

Command Syntax and Usage
addr *<IP address>* Configures the IP address for the Backup Switch Interface, using dotted decimal notation.
mask *<subnet mask>* Configures the IP subnet address mask for the interface, using dotted decimal notation.
vlan *<1-4095>* Configures the VLAN number for this interface.
gw *<IP address>* Configures the default gateway for the Backup Switch Interface.
del Deletes the Backup Switch Interface.
cur Displays the current Backup Switch Interface parameters.

/cfg/pmirr
Port Mirroring Configuration

```
[Port Mirroring Menu]
      mirror  - Enable/Disable Mirroring
      monport - Monitoring Port based PM Menu
      cur     - Display All Mirrored and Monitoring Ports
```

Port mirroring is disabled by default. For more information about port mirroring on the switch, see "Appendix A: Troubleshooting" in the BLADE OS *Application Guide*.

NOTE – Traffic on VLAN 4095 is not mirrored to the external ports.

The Port Mirroring Menu is used to configure, enable, and disable the monitored port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

Table 6-30 Port Mirroring Menu Options (/cfg/pmirr)

Command Syntax and Usage
mirror disable|enable Enables or disables port mirroring
monport *<port number>* Displays port-mirroring menu. To view menu options, see page 155.
cur Displays current settings of the mirrored and monitoring ports.

/cfg/pmirr/monport
Port-Mirroring Configuration

```
[Port 2:1 Menu]
     add      - Add "Mirrored" port
     rem      - Rem "Mirrored" port
     delete   - Delete this "Monitor" port
     cur      - Display current Port-based Port Mirroring configuration
```

Table 6-31 Port Mirroring Monitor Port Menu Options (/cfg/pmirr/monport)

Command Syntax and Usage
add *<mirrored port (port to mirror from)> <direction (in, out, or both)>* Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because: If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the mirrored port. If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.
rem *<mirrored port (port to mirror from)>* Removes the mirrored port.
delete Deletes this monitor port.
cur Displays the current settings of the monitoring port.

/cfg/l2
Layer 2 Configuration

```
[Layer 2 Menu]
     8021x    - 802.1X Menu
     fdb      - FDB Menu
     trunk    - Trunk Group Menu
     thash    - IP Trunk Hash Menu
     lacp     - Link Aggregation Control Protocol Menu
     failovr  - Failover Menu
     vlan     - VLAN Menu
     bpdugrd  - Enable/disable BPDU Guard
     cur      - Display current layer 2 parameters
```

Table 6-32 Layer 2 Configuration Menu (/cfg/l2)

Command Syntax and Usage
8021x Displays the 802.1X Configuration Menu. To view menu options, see page 157.
fdb Displays the Forwarding Database Menu. To view menu options, see page 163.
trunk *<trunk number>* Displays the Trunk Group Configuration Menu. To view menu options, see page 164.
thash Displays the IP Trunk Hash Menu. To view menu options, see page 165.
lacp Displays the Link Aggregation Control Protocol Menu. To view menu options, see page 167.
failovr Displays the Failover Configuration Menu. To view menu options, see page 169.
vlan *<VLAN number (1-4095)>* Displays the VLAN Configuration Menu. To view menu options, see page 174.
bpdugrd enable|disable Globally enables or disables BPDU Guard. If Spanning Tree BPDUs are received on a port, BPDU Guard disables the port.
cur Displays current Layer 2 parameters.

/cfg/l2/8021x
802.1X Configuration

```
[802.1X Configuration Menu]
     global   - Global 802.1X configuration menu
     port     - Port 802.1X configuration menu
     ena      - Enable 802.1X access control
     dis      - Disable 802.1X access control
     cur      - Show 802.1X configuration
```

This feature allows you to configure the switch as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 6-33 802.1X Configuration Menu (/cfg/l2/8021x)

Command Syntax and Usage
global Displays the global 802.1X Configuration Menu. To view menu options, see page 158.
port *<port number>* Displays the 802.1X Port Menu. To view menu options, see page 161.
ena Globally enables 802.1X.
dis Globally disables 802.1X.
cur Displays current 802.1X parameters.

/cfg/l2/8021x/global
802.1X Global Configuration

```
[802.1X Global Configuration Menu]
     gvlan    - 802.1X Guest VLAN configuration menu
     mode     - Set access control mode
     qtperiod - Set EAP-Request/Identity quiet time interval
     txperiod - Set EAP-Request/Identity retransmission timeout
     suptmout - Set EAP-Request retransmission timeout
     svrtmout - Set server authentication request timeout
     maxreq   - Set max number of EAP-Request retransmissions
     raperiod - Set reauthentication time interval
     reauth   - Set reauthentication status to on or off
     vassign  - Set dynamic VLAN assignment status to on or off
     default  - Restore default 802.1X configuration
     cur      - Display current 802.1X configuration
```

The global 802.1X menu allows you to configure parameters that affect all ports in the switch.

Table 6-34 802.1X Global Configuration Menu Options (/cfg/l2/8021x/global)

Command Syntax and Usage
gvlan Displays the 802.1X Guest VLAN Configuration Menu. To view menu options, see page 160.
mode force-unauth|auto|force-auth Sets the type of access control for all ports: ■ **force-unauth** - the port is unauthorized unconditionally. ■ **auto** - the port is unauthorized until it is successfully authorized by the RADIUS server. ■ **force-auth** - the port is authorized unconditionally, allowing all traffic. The default value is `force-auth`.
qtperiod *<0-65535>* Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.
txperiod *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.
suptmout *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.

Table 6-34 802.1X Global Configuration Menu Options (/cfg/l2/8021x/global)

Command Syntax and Usage
svrtmout *<1-65535>* Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of `/cfg/sys/radius/timeout` (default is 3 seconds).
maxreq *<1-10>* Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.
raperiod *<1-604800>* Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.
reauth on|off Sets the re-authentication status to `on` or `off`. The default value is `off`.
vassign on|off Globally sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`. This feature allows the RADIUS server to specify the VLAN for the port during 802.1x authentication.
default Resets the global 802.1X parameters to their default values.
cur Displays current global 802.1X parameters.

/cfg/l2/8021x/global/gvlan
802.1X Guest VLAN Configuration

```
[802.1X Guest VLAN Configuration Menu]
     vlan     - Set 8021.x Guest VLAN number
     ena      - Enable 8021.xGuest VLAN
     dis      - Disable 8021.x Guest VLAN
     cur      - Display current Guest VLAN configuration
```

The 802.1X Guest VLAN menu allows you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

Table 6-35 802.1X Guest VLAN Configuration Menu (/cfg/l2/8021x/global/gvlan)

Command Syntax and Usage
vlan *<1-4094>* Configures the Guest VLAN number.
ena Enables the 802.1X Guest VLAN.
dis Disables the 802.1X Guest VLAN.
cur Displays current 802.1X Guest VLAN parameters.

/cfg/l2/8021x/port *<alias or number>*
802.1X Port Configuration

```
[802.1X Port Configuration Menu]
    mode     - Set access control mode
    qtperiod - Set EAP-Request/Identity quiet time interval
    txperiod - Set EAP-Request/Identity retransmission timeout
    suptmout - Set EAP-Request retransmission timeout
    svrtmout - Set server authentication request timeout
    maxreq   - Set max number of EAP-Request retransmissions
    raperiod - Set reauthentication time interval
    reauth   - Set reauthentication status to on or off
    vassign  - Set dynamic VLAN assignment status to on or off
    default  - Restore default 802.1X configuration
    global   - Apply current global 802.1X configuration to this port
    cur      - Display current 802.1X configuration
```

The 802.1X port menu allows you to configure parameters that affect the selected port in the switch. These settings override the global 802.1X parameters.

Table 6-36 802.1X Port Configuration Menu Options (/cfg/l2/8021x/port)

Command Syntax and Usage
mode force-unauth|auto|force-auth Sets the type of access control for the port: ■ **force-unauth** - the port is unauthorized unconditionally. ■ **auto** - the port is unauthorized until it is successfully authorized by the RADIUS server. ■ **force-auth** - the port is authorized unconditionally, allowing all traffic. The default value is `force-auth`.
qtperiod *<0-65535>* Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.
txperiod *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.
suptmout *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.

Table 6-36 802.1X Port Configuration Menu Options (/cfg/l2/8021x/port)

Command Syntax and Usage
svrtmout *<1-65535>* Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of `/cfg/sys/radius/timeout` (default is 3 seconds).
maxreq *<1-10>* Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.
raperiod *<1-604800>* Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.
reauth on|off Sets the re-authentication status to `on` or `off`. The default value is `off`.
vassign on|off Sets the dynamic VLAN assignment for the selected port to `on` or `off`. The default value is `off`. This feature allows the RADIUS server to specify the VLAN for the port during 802.1x authentication.
default Resets the 802.1X port parameters to their default values.
global Applies current global 802.1X configuration parameters to the port.
cur Displays current 802.1X port parameters.

/cfg/l2/fdb
Forwarding Database Configuration

```
[FDB Menu]
     aging    - Configure FDB aging value
     cur      - Display current FDB configuration
```

Use the following commands to configure the Forwarding Database (FDB) for the G8000.

Table 6-37 FDB Menu Options (/cfg/l2/fdb)

Command Syntax and Usage
aging *<0-65535>* Configures the aging value for FDB entries, in seconds. The default value is 300.
cur Displays the current FDB parameters.

/cfg/l2/trunk <trunk group number>
Trunk Configuration

```
[Trunk group 1 Menu]
      add     - Add port to trunk group
      rem     - Remove port from trunk group
      ena     - Enable trunk group
      dis     - Disable trunk group
      del     - Delete trunk group
      cur     - Display current Trunk Group configuration
```

Trunk groups can provide super-bandwidth connections between switches or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. The following restrictions apply to trunk group configuration:

- Any physical switch port can belong to no more than one trunk group.
- Up to eight ports can belong to the same trunk group.
- Configure all ports in a trunk group with the same link configuration (speed, duplex, flow control).
- Trunking from non-BLADE devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 6-38 Trunk Configuration Menu Options (/cfg/l2/trunk)

Command Syntax and Usage
add <*port number*> Adds a physical port to the current trunk group.
rem <*port number*> Removes a physical port from the current trunk group.
ena Enables the current trunk group.
dis Disables the current trunk group.
del Removes the current trunk group configuration.
cur Displays current trunk group parameters.

/cfg/l2/thash
IP Trunk Hash Configuration

```
[IP Trunk Hash Menu]
     set       - IP Trunk Hash Settings Menu
     cur       - Display current IP trunk hash configuration
```

Use the following commands to configure IP trunk hash settings for the switch. The trunk hash settings affect both static trunks and LACP trunks.

Table 6-39 IP Trunk Hash Menu Options (/cfg/l2/thash)

Command Syntax and Usage
set Displays the Trunk Hash Settings menu. To view menu options, see page 165.
cur Display current trunk hash configuration.

/cfg/l2/thash/set
IP Trunk Hash

```
[set IP Trunk Hash Settings Menu]
     smac      - Enable/disable smac hash
     dmac      - Enable/disable dmac hash
     sip       - Enable/disable sip hash
     dip       - Enable/disable dip hash
     cur       - Display current trunk hash setting
```

Trunk hash parameters are set globally for the switch. You can enable one or two parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

Use the following commands to configure IP trunk hash parameters for the switch.

Table 6-40 IP Trunk Hash Menu Options (/cfg/l2/thash/set)

Command Syntax and Usage
smac enable|**disable** Enable or disable trunk hashing on the source MAC.
dmac enable|**disable** Enable or disable trunk hashing on the destination MAC.
sip enable|**disable** Enable or disable trunk hashing on the source IP.
dip enable|**disable** Enable or disable trunk hashing on the destination IP.
cur Display current layer 2 trunk hash setting.

/cfg/l2/lacp
LACP Configuration

```
[LACP Menu]
     sysprio  - Set LACP system priority
     timeout  - Set LACP system timeout scale for timing out partner
                info
     port     - LACP port Menu
     cur      - Display current LACP configuration
```

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the switch.

Table 6-41 LACP Menu Options (/cfg/l2/lacp)

Command Syntax and Usage
sysprio *<1-65535>* Defines the priority value (1 through 65535) for the switch. Lower numbers provide higher priority. The default value is 32768.
timeout short|long Defines the timeout period before invalidating LACP data from a remote partner. Choose **short** (3 seconds) or **long** (90 seconds). The default value is **long**. **Note**: It is recommended that you use a timeout value of **long**, to reduce LACPDU processing. If your switch's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.
port *<port number>* Displays the LACP Port menu. To view menu options, see page 168.
cur Display current LACP configuration.

/cfg/l2/lacp/port <port number>
LACP Port Configuration

```
[LACP Port 2:1 Menu]
     mode     - Set LACP mode
     prio     - Set LACP port priority
     adminkey - Set LACP port admin key
     cur      - Display current LACP port configuration
```

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the selected port.

Table 6-42 LACP Port Menu Options (/cfg/l2/lacp/port)

Command Syntax and Usage
mode off|active|passive Set the LACP mode for this port, as follows: ■ **off** Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is **off**. ■ **active** Turn LACP on and set this port to active. Active ports initiate LACPDUs. ■ **passive** Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.
prio *<1-65535>* Sets the priority value for the selected port. Lower numbers provide higher priority. Default is 32768.
adminkey *<1-65535>* Set the admin key for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group.
cur Displays the current LACP configuration for this port.

/cfg/l2/failovr
Layer 2 Failover Configuration

```
[Failover Menu]
     trigger  - Trigger Menu
     on       - Globally turn Failover ON
     off      - Globally turn Failover OFF
     cur      - Display current Failover configuration
```

Use this menu to configure Layer 2 Failover. For more information about Layer 2 Failover, see "High Availability" in the BLADE OS *Application Guide*.

Table 6-43 Layer 2 Failover Menu Options (/cfg/l2/failovr)

Command Syntax and Usage
trigger *<1-8>* Displays the Failover Trigger menu. To view menu options, see page 170.
on Globally turns Layer 2 failover `on`.
off Globally turns Layer 2 failover `off`.
cur Displays current Layer 2 failover parameters.

/cfg/l2/failovr/trigger
Failover Trigger Configuration

```
[Trigger 1 Menu]
     mmon      - Manual Monitor Menu
     limit     - Limit of Trigger
     ena       - Enable Trigger
     dis       - Disable Trigger
     del       - Delete Trigger
     cur       - Display current Trigger configuration
```

Table 6-44 Failover Trigger Menu Options (/cfg/l2/failovr/trigger)

Command Syntax and Usage
mmon Displays the Manual Monitor menu for the selected trigger. To view menu options, see page 171.
limit *<0-1024>* Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational.
ena Enables the selected trigger.
dis Disables the selected trigger.
cur Displays the current failover trigger settings.

/cfg/l2/failovr/trigger/mmon
Manual Monitor Configuration

```
[Manual Monitor Menu]
     monitor  - Monitor Menu
     control  - Control Menu
     cur      - Display current Manual Monitor configuration
```

Table 6-45 Manual Monitor Menu Options (/cfg/l2/failovr/trigger/mmon)

Command Syntax and Usage
monitor Displays the Manual Monitor-Monitor menu. To view menu options, see page 172.
control Displays the Manual Monitor-Control menu. To view menu options, see page 173.
cur Displays the current Manual Monitor settings.

/cfg/l2/failovr/trigger/mmon/monitor
Manual Monitor-Monitor Configuration

```
[Monitor Menu]
     addport  - Add port to Monitor
     remport  - Remove port from Monitor
     addtrnk  - Add trunk to Monitor
     remtrnk  - Remove trunk from Monitor
     addkey   - Add LACP port adminkey to Monitor
     remkey   - Remove LACP port adminkey from Monitor
     cur      - Display current Monitor configuration
```

Table 6-46 Manual Monitor-Monitor options (/cfg/l2/failovr/trigger/mmon/monitor)

Command Syntax and Usage
addport *<port number>* Adds the selected port to the Manual Monitor - Monitor.
remport *<port number>* Removes the selected port from the Manual Monitor - Monitor.
addtrnk *<trunk number)>* Adds a trunk group to the Manual Monitor - Monitor.
remtrnk *<trunk number>* Removes a trunk group from the Manual Monitor - Monitor.
addkey *<1-65535>* Adds an LACP admin key to the Manual Monitor - Monitor. LACP trunks formed with this admin key will be included in the Manual Monitor - Monitor.
remkey *<1-65535>* Removes an LACP admin key from the Manual Monitor - Monitor.
cur Displays the current Manual Monitor - Monitor configuration.

/cfg/l2/failovr/trigger/mmon/control
Manual Monitor-Control Configuration

```
[Control Menu]
     addport  - Add port to Control
     remport  - Remove port from Control
     addtrnk  - Add trunk to Control
     remtrnk  - Remove trunk from Control
     addkey   - Add LACP port adminkey to Control
     remkey   - Remove LACP port adminkey from Control
     cur      - Display current Control configuration
```

Table 6-47 Manual Monitor-Control options (/cfg/l2/failovr/trigger/mmon/control)

Command Syntax and Usage
addport *<port number>* Adds the selected port to the Manual Monitor - Control.
remport *<port number>* Removes the selected port from the Manual Monitor - Control.
addtrnk *<trunk number)>* Adds a trunk group to the Manual Monitor - Control.
remtrnk *<trunk number>* Removes a trunk group from the Manual Monitor - Control.
addkey *<1-65535>* Adds a LACP admin key to the Manual Monitor - Control. LACP trunks formed with this admin key will be included in the Manual Monitor - Control.
remkey *<1-65535>* Removes a LACP admin key from the Manual Monitor - Control.
cur Displays the current Manual Monitor - Control configuration.

/cfg/l2/vlan <VLAN number>
VLAN Configuration

```
[VLAN 1 Menu]
     name     - Set VLAN name
     add      - Add port to VLAN
     rem      - Remove port from VLAN
     def      - Define VLAN as list of ports
     ena      - Enable VLAN
     dis      - Disable VLAN
     del      - Delete VLAN
     cur      - Display current VLAN configuration
```

The commands in this menu configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs.

By default, the VLAN menu option is disabled except VLAN 1, which is enabled all the time. Up to 1024 VLANs can be configured on the switch.

Table 6-48 VLAN Configuration Menu Options (/cfg/l2/vlan)

Command Syntax and Usage
name Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.
add *<port number>* Adds port(s) to the VLAN membership.
rem *<port number>* Removes port(s) from this VLAN.
def *<list of port numbers>* Defines which ports are members of this VLAN. Every port must be a member of at least one VLAN.
ena Enables this VLAN.
dis Disables this VLAN without removing it from the configuration.
del Deletes this VLAN.
cur Displays the current VLAN configuration.

NOTE – All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on (see the `tag` command on page 146).

/cfg/l3
Layer 3 Configuration

```
[Layer 3 Menu]
     igmp      - IGMP Menu
     dns       - Domain Name System Menu
     rearp     - Set re-ARP period in minutes
     cur       - Display current IP configuration
```

Table 6-49 Layer 3 Configuration Menu (/cfg/l3)

Command Syntax and Usage
igmp Displays the IGMP Menu. To view menu options, see page 177.
dns Displays the IP Domain Name System Menu. To view menu options, see page 184.
rearp *<2-120>* Defines re-ARP period in minutes. You can set this duration between 2 and 120 minutes.
cur Displays the current IP configuration.

/cfg/l3/igmp
IGMP Configuration

```
[IGMP Menu]
     snoop    - IGMP Snoop Menu
     mrouter  - Static Multicast Router Menu
     igmpflt  - IGMP Filtering Menu
     on       - Globally turn IGMP ON
     off      - Globally turn IGMP OFF
     cur      - Display current IGMP configuration
```

Table 6-50 describes the commands used to configure basic IGMP parameters.

Table 6-50 IGMP Menu Options (/cfg/l3/igmp)

Command Syntax and Usage
snoop Displays the IGMP Snoop Menu. To view menu options, see page 178.
mrouter Displays the Static Multicast Router Menu. To view menu options, see page 180.
igmpflt Displays the IGMP Filtering Menu. To view menu options, see page 181.
on Globally turns IGMP on.
off Globally turns IGMP off.
cur Displays the current IGMP configuration parameters.

/cfg/l3/igmp/snoop
IGMP Snooping Configuration

```
[IGMP Snoop Menu]
     timeout  - Set report timeout
     mrto     - Set multicast router timeout
     qintrval - Set IGMP query interval
     robust   - Set expected packet loss on subnet
     flood    - Flood unregistered IPMC
     cpu      - Send unregistered IPMC to CPU
     aggr     - Aggregate IGMP report
     srcip    - Set source ip to use when proxying GSQ
     add      - Add VLAN(s) to IGMP Snooping
     rem      - Remove VLAN(s) from IGMP Snooping
     clear    - Remove all VLAN(s) from IGMP Snooping
     fastlv   - Enable/disable Fastleave processing in VLAN
     def      - Set IGMP Snooping settings to factory default
     cur      - Display current IGMP Snooping configuration
```

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

Table 6-51 describes the commands used to configure IGMP Snooping.

Table 6-51 IGMP Snoop Menu Options (/cfg/l3/igmp/snoop)

Command Syntax and Usage
timeout *<1-255 seconds>* Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is 10 seconds.
mrto *<1-600 seconds>* Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is 255 seconds.
qinterval *<1-600>* Configures the interval for IGMP Query Reports. The default value is 125 seconds.
robust *<2-10>* Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2.

Table 6-51 IGMP Snoop Menu Options (/cfg/l3/igmp/snoop)

Command Syntax and Usage
flood enable|disable Configures the switch to flood unregistered IP multicast reports to all ports. The default setting is `enabled`. **Note:** If IGMP hosts reside on different VLANs, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs.
cpu enable|disable Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows: ■ If no Mrouter is present, drop subsequent packets with same IPMC. ■ If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN. The default setting is `enabled`. **Note**: If both **flood** and **cpu** are disabled, then the switch drops all unregistered IPMC traffic.
aggr enable|disable Enables or disables IGMP Membership Report aggregation.
srcip *<IP address (such as, 192.4.17.101)>* Configures the source IP address used as a proxy for IGMP Group Specific Queries.
add *<VLAN number (1-4094)>* Adds the selected VLAN(s) to IGMP Snooping.
rem *<VLAN number (1-4094)>* Removes the selected VLAN(s) from IGMP Snooping.
clear Removes all VLANs from IGMP Snooping.
fastlv *<VLAN number (1-4094)>* **disable|enable** Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default.
def Resets IGMP Snooping parameters to their default values.
cur Displays the current IGMP Snooping parameters.

/cfg/l3/igmp/mrouter

IGMP Static Multicast Router Configuration

```
[Static Multicast Router Menu]
      add     - Add port as Multicast Router Port
      rem     - Remove port as Multicast Router Port
      cur     - Display current Multicast Router configuration
```

Table 6-52 describes the commands used to configure a static multicast router.

NOTE – When you configure a static multicast router on a VLAN, the process of learning multicast routers is disabled for that VLAN.

Table 6-52 IGMP Static Multicast Router Menu Options (/cfg/l3/igmp/mrouter)

Command Syntax and Usage
add *<port number> <VLAN number> <IGMP version number>* Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1, 2, or 3) of the multicast router.
remove *<port number> <VLAN number> <IGMP version number>* Removes a static multicast router from the selected port/VLAN combination.
cur Displays the current IGMP Static Multicast Router parameters.

/cfg/l3/igmp/igmpflt
IGMP Filtering Configuration

```
[IGMP Filter Menu]
      filter  - IGMP Filter Definition Menu
      port    - IGMP Filtering Port Menu
      ena     - Enable IGMP Filtering
      dis     - Disable IGMP Filtering
      cur     - Display current IGMP Filtering configuration
```

Table 6-53 describes the commands used to configure an IGMP filter.

Table 6-53 IGMP Filtering Menu Options (/cfg/l3/igmp/igmpflt)

Command Syntax and Usage
filter *<filter number (1-16)>* Displays the IGMP Filter Definition Menu. To view menu options, see page 182.
port *<port number>* Displays the IGMP Filtering Port Menu. To view menu options, see page 183.
ena Enables IGMP filtering globally.
dis Disables IGMP filtering globally.
cur Displays the current IGMP Filtering parameters.

/cfg/l3/igmp/igmpflt/filter <filter number>
IGMP Filter Definition

```
[IGMP Filter 1 Definition Menu]
      range   - Set IP Multicast address range
      action  - Set filter action
      ena     - Enable filter
      dis     - Disable filter
      del     - Delete filter
      cur     - Display current IGMP filter configuration
```

Table 6-54 describes the commands used to define an IGMP filter.

Table 6-54 IGMP Filter Definition Menu Options (/cfg/l3/igmp/igmpflt/filter)

Command Syntax and Usage
range *<IP multicast address (such as 224.0.0.10)> <IP multicast address>* Configures the range of IP multicast addresses for this filter.
action allow|deny Allows or denies multicast traffic for the IP multicast addresses specified.
ena Enables this IGMP filter.
dis Disables this IGMP filter.
del Deletes this filter's parameter definitions.
cur Displays the current IGMP filter.

/cfg/l3/igmp/igmpflt/port <port number>
IGMP Filtering Port Configuration

```
[IGMP Port 1:1 Menu]
      filt    - Enable/disable IGMP filtering on port
      add     - Add IGMP filter to port
      rem     - Remove IGMP filter from port
      cur     - Display current IGMP filtering Port configuration
```

Table 6-55 describes the commands used to configure a port for IGMP filtering.

Table 6-55 IGMP Filter Port Menu Options (/cfg/l3/igmp/igmpflt/port)

Command Syntax and Usage
filt enable|disable Enables or disables IGMP filtering on this port.
add *<filter number (1-16)>* Adds an IGMP filter to this port.
rem *<filter number (1-16)>* Removes an IGMP filter from this port.
cur Displays the current IGMP filter parameters for this port.

/cfg/l3/dns
Domain Name System Configuration

```
[Domain Name System Menu]
      prima   - Set IP address of primary DNS server
      secon   - Set IP address of secondary DNS server
      dname   - Set default domain name
      cur     - Display current DNS configuration
```

The Domain Name System (DNS) Menu is used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `traceroute`, and `tftp` commands.

Table 6-56 Domain Name Service Menu Options (/cfg/l3/dns)

Command Syntax and Usage
prima *<IP address (such as 192.4.17.101)>* You will be prompted to set the IP address for your primary DNS server. Use dotted decimal notation.
secon *<IP address (such as 192.4.17.101)>* You will be prompted to set the IP address for your secondary DNS server. If the primary DNS server fails, the configured secondary will be used instead. Enter the IP address using dotted decimal notation.
dname *<dotted DNS notation>* | **none** Sets the default domain name used by the switch. For example: `mycompany.com`
cur Displays the current Domain Name System settings.

/cfg/qos
Quality of Service Configuration

```
[QOS Menu]
     8021p     - 802.1p Menu
     dscp      - Dscp Menu
```

Use the Quality of Service (QoS) menus to configure the 802.1p priority value and DiffServ Code Point (DSCP) value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

Table 6-57 Quality of Service Menu Options (/cfg/qos)

Command Syntax and Usage
8021p Displays 802.1p configuration menu. To view menu options, see page 186.
dscp Displays DSCP configuration menu. To view menu options, see page 187.

/cfg/qos/8021p
802.1p Configuration

```
[802.1p Menu]
     priq      - Set priority to COS queue mapping
     qweight   - Set weight to a COS queue
     numcos    - Set number of COS queue
     default   - Reset 802.1p configuration to default values.
     cur       - Display current 802.1p configuration
```

This feature provides the capability to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

Table 6-58 802.1p Menu Options (/cfg/qos/8021p)

Command Syntax and Usage
priq *<0-7>* **{***<COSq number>***}** Maps the 802.1p priority to the Class of Service queue (COSq) number. Enter the 802.1p priority value, followed by the Class of Service queue that handles the matching traffic. Note that priority value 7 is reserved for Stacking.
qweight {*<COSq number>***}** *<0-15>* Configures the weight of the selected Class of Service queue (COSq). Enter the queue number, followed by the scheduling weight (0-15).
numcos 1|7 Sets the number of Class of Service queues for switch ports. Note that one COSq is reserved for Stacking.
default Resets 802.1p parameters to their default values.
cur Displays the current 802.1p parameters.

/cfg/qos/dscp
DSCP Configuration

```
[dscp Menu]
     dscp      - Remark DSCP value to a new DSCP value
     prio      - Remark DSCP value to a 802.1p priority
     on        - Globally turn DSCP remarking ON
     off       - Globally turn DSCP remarking OFF
     cur       - Display current DSCP remarking configuration
```

Use this menu map the DiffServ Code Point (DSCP) value of incoming packets to a new value, or to an 802.1p priority value.

Table 6-59 DSCP Menu Options (/cfg/qos/dscp)

Command Syntax and Usage
dscp *<0-63> <0-63>* Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value (0-63) of incoming packets, followed by the new value.
prio *<dscp (0-63)> <priority (0-7)>* Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value.
on Turns on DSCP re-marking globally.
off Turns off DSCP re-marking globally.
cur Displays the current DSCP parameters.

/cfg/acl
Access Control List Configuration

```
[ACL Menu]
     acl       - Access Control List Item Config Menu
     group     - Access Control List Group Config Menu
     cur       - Display current ACL configuration
```

Use this menu to create Access Control Lists and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

Table 6-60 ACL Menu Options (/cfg/acl)

Command Syntax and Usage
acl *<1-768>* Displays Access Control List configuration menu. To view menu options, see page 189.
group *<1-768>* Displays ACL Group configuration menu. To view menu options, see page 199.
cur Displays the current ACL parameters.

/cfg/acl/acl <ACL number>
ACL Configuration

```
[ACL 1 Menu]
     ethernet - Ethernet Header Options Menu
     ipv4     - IP Header Options Menu
     tcpudp   - TCP/UDP Header Options Menu
     meter    - ACL Metering Configuration Menu
     re-mark  - ACL Re-mark Configuration Menu
     pktfmt   - Set to filter specific packet format types
     egrport  - Set to filter for packets egressing this port
     action   - Set filter action
     stats    - Enable/disable statistics for this acl
     reset    - Reset filtering parameters
     cur      - Display current filter configuration
```

These menus allow you to define filtering criteria for each Access Control List (ACL).

Table 6-61 ACL Menu Options (/cfg/acl/acl x)

Command Syntax and Usage
ethernet Displays the ACL Ethernet Header menu. To view menu options, see page 190.
ipv4 Displays the ACL IP Header menu. To view menu options, see page 191.
tcpudp Displays the ACL TCP/UDP Header menu. To view menu options, see page 193.
meter Displays the ACL Metering menu. To view menu options, see page 194.
re-mark Displays the ACL Re-mark menu. To view menu options, see page 195.
pktfmt *<packet format>* Displays the ACL Packet Format menu. To view menu options, see page 198.
egrport *<port number>* Configures the ACL to function on egress packets.
action permit|deny|setprio *<0-7>* Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).

Table 6-61 ACL Menu Options (/cfg/acl/acl x)

Command Syntax and Usage
stats enable|**disable** Enables or disables the statistics collection for the Access Control List.
reset Resets the ACL parameters to their default values.
cur Displays the current ACL parameters.

/cfg/acl/acl *<ACL number>*/ethernet
Ethernet Filtering Configuration

```
      smac      - Set to filter on source MAC
      dmac      - Set to filter on destination MAC
      vlan      - Set to filter on VLAN ID
      etype     - Set to filter on ethernet type
      pri       - Set to filter on priority
      reset     - Reset all fields
      cur       - Display current parameters
```

This menu allows you to define Ethernet matching criteria for an ACL.

Table 6-62 Ethernet Filtering Menu Options (/cfg/acl/acl x/ethernet)

Command Syntax and Usage
smac *<MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>* Defines the source MAC address for this ACL.
dmac *<MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>* Defines the destination MAC address for this ACL.
vlan *<1-4095> <VLAN mask (0xfff)>* Defines a VLAN number and mask for this ACL.
etype ARP|**IP**|**IPv6**|**MPLS**|**RARP**|**any**|**0xXXXX** Defines the Ethernet type for this ACL.
pri *<0-7>* Defines the Ethernet priority value for the ACL.

Table 6-62 Ethernet Filtering Menu Options (/cfg/acl/acl x/ethernet)

Command Syntax and Usage
reset Resets Ethernet parameters for the ACL to their default values.
cur Displays the current Ethernet parameters for the ACL.

/cfg/acl/acl *<ACL number>*/ipv4
IP version 4 Filtering Configuration

```
[Filtering IPv4 Menu]
     sip       - Set to filter on source IP address
     dip       - Set to filter on destination IP address
     proto     - Set to filter on prototype
     tos       - Set to filter on TOS
     reset     - Reset all fields
     cur       - Display current parameters
```

This menu allows you to define IPv4 matching criteria for an ACL.

Table 6-63 IP version 4 Filtering Menu Options (/cfg/acl/acl x/ipv4)

Command Syntax and Usage
sip *<IP address> <mask (such as 255.255.255.0)>* Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.
dip *<IP address> <mask (such as 255.255.255.0)>* Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.
proto *<0-255>* Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols. **Number** **Name** 1 icmp 2 igmp 6 tcp 17 udp

Table 6-63 IP version 4 Filtering Menu Options (/cfg/acl/acl x/ipv4)

Command Syntax and Usage
tos *<0-255>* Defines a Type of Service value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.
reset Resets the IPv4 parameters for the ACL to their default values.
cur Displays the current IPV4 parameters.

/cfg/acl/acl <ACL number>/tcpudp
TCP/UDP Filtering Configuration

```
[Filtering TCP/UDP Menu]
     sport    - Set to filter on TCP/UDP source port
     dport    - Set to filter on TCP/UDP destination port
     flags    - Set to filter TCP/UDP flags
     reset    - Reset all fields
     cur      - Display current parameters
```

This menu allows you to define TCP/UDP matching criteria for an ACL.

Table 6-64 TCP/UDP Filtering Menu Options (/cfg/acl/acl x/tcpudp)

Command Syntax and Usage
sport *<source port (1-65535)> <mask (0xFFFF)>* Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports: **Number** — **Name** **20** ftp-data **21** ftp **22** ssh **23** telnet **25** smtp **37** time **42** name **43** whois **53** domain **69** tftp **70** gopher **79** finger **80** http
dport *<destination port (1-65535)> <mask (0xFFFF)>* Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with `sport` above.
flags *<value (0x0-0x3f)>* Defines a TCP/UDP flag for the ACL.

Table 6-64 TCP/UDP Filtering Menu Options (/cfg/acl/acl x/tcpudp)

Command Syntax and Usage
reset Resets the TCP/UDP parameters for the ACL to their default values.
cur Displays the current TCP/UDP Filtering parameters.

/cfg/acl/acl *<ACL number>*/meter
ACL Metering Configuration

```
[Metering Menu]
     cir       - Set committed rate in KiloBits/s
     mbsize    - Set maximum burst size in KiloBits
     enable    - Enable/disable port metering
     dpass     - Set to Drop or Pass out of profile traffic
     reset     - Reset meter parameters
     cur       - Display current settings
```

This menu defines the metering profile for the selected ACL.

Table 6-65 ACL Metering Menu Options (/cfg/acl/acl x/meter)

Command Syntax and Usage
cir *<64-10000000>* Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64.
mbsize *<32-4096>* Configures the maximum burst size, in Kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096
enable e|d Enables or disables metering on the ACL.
dpass drop|pass Configures the ACL Meter to either drop or pass out-of-profile traffic.
reset Reset ACL Metering parameters to their default values.
cur Displays current ACL Metering parameters.

/cfg/acl/acl <ACL number>/re-mark
Re-Mark Configuration

```
[Re-mark Menu]
     inprof   - In Profile Menu
     outprof  - Out Profile Menu
     up1p     - Set Update User Priority Menu
     reset    - Reset re-mark settings
     cur      - Display current settings
```

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL Metering profile, or out of the ACL Metering profile.

Table 6-66 ACL Re-mark Menu Options (/cfg/acl/acl x/re-mark)

Command Syntax and Usage
inprof Displays the Re-mark In-Profile Menu. To view menu options, see page 196.
outprof Displays the Re-mark Out-of-Profile Menu. To view menu options, see page 196.
up1p Displays the Re-Mark In-Profile Update User Priority Menu. To view menu options, see page 197.
reset Reset ACL Re-mark parameters to their default values.
cur Displays current Re-mark parameters.

/cfg/acl/acl <ACL number>/re-mark/inprof
Re-Marking In-Profile Configuration

```
[Re-marking - In Profile Menu]
     updscp    - Set the update DSCP
     reset     - Reset update DSCP settings
     cur       - Display current settings
```

Table 6-67 ACL Re-Mark In-Profile Menu (/cfg/acl/acl x/re-mark/inprof)

Command Syntax and Usage
updscp *<0-63>* Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value.
reset Resets the update DSCP parameters to their default values.
cur Displays current Re-Mark In-Profile parameters.

/cfg/acl/acl <ACL number>/re-mark/outprof
Re-Marking Out-of-Profile Configuration

```
[Re-marking - Out Of Profile Menu]
     updscp    - Set the update DSCP
     reset     - reset update DSCP setting
     cur       - Display current settings
```

Table 6-68 ACL Re-Mark Out-of-Profile Menu (/cfg/acl/acl x/re-mark/outprof)

Command Syntax and Usage
updscp *<0-63>* Sets the DiffServ Code Point (DSCP) of Out-of-Profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets.
reset Resets the update DSCP parameters for Out-of-Profile packets to their default values.
cur Displays current Re-Mark Out-of-Profile parameters.

/cfg/acl/acl <ACL number>/re-mark/inprof/up1p
Update User Priority Configuration

```
[Update User Priority Menu]
     value    - Set the update user priority
     utosp    - Enable/Disable use of TOS precedence
     reset    - Reset in profile up1p settings
     cur      - Display current settings
```

Table 6-69 ACL Re-Mark User Priority Menu (/cfg/acl/acl x/re-mark/inprof/up1p)

Command Syntax and Usage
value *<0-7>* Defines 802.1p value. The value is the priority bits information in the packet structure.
utosp enable|**disable** Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value.
reset Resets UP1P settings to their default values.
cur Displays current Re-Mark In-Profile User Priority parameters.

/cfg/acl/acl <ACL number>/pktfmt
Packet Format Filtering Configuration

```
[Filtering Packet Format Menu]
     ethfmt    - Set to filter on ethernet format
     tagfmt    - Set to filter on ethernet tagging format
     ipfmt     - Set to filter on IP format
     reset     - Reset all fields
     cur       - Display current parameters
```

This menu allows you to define Packet Format matching criteria for an ACL.

Table 6-70 ACL Packet Format Filtering Menu Options (/cfg/acl/acl x/pktfmt)

Command Syntax and Usage
ethfmt eth2|SNAP|LLC Defines the Ethernet format for the ACL.
tagfmt none|tagged Defines the tagging format for the ACL.
ipfmt none|v4|v6 Defines the IP format for the ACL.
reset Resets Packet Format parameters for the ACL to their default values.
cur Displays the current Packet Format parameters for the ACL.

/cfg/acl/group *<ACL Group number>*
ACL Group Configuration

```
[ACL Group 1 Menu]
     add       - Add ACL to group
     rem       - Remove ACL from group
     cur       - Display current ACL items in group
```

This menu allows you to compile one or more ACLs into an ACL Group. Once you create an ACL Group, you can assign the ACL Group to one or more ports.

Table 6-71 ACL Group Menu Options (/cfg/acl/group x)

Command Syntax and Usage
add acl *<1-768>* Adds the selected ACL to the ACL Group.
rem acl *<1-768>* Removes the selected ACL from the ACL Group.
cur Displays the current ACL group parameters.

/cfg/dump
Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the `Configuration#` prompt, enter:

```
Configuration# dump
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via TFTP, as described on page 200.

/cfg/ptcfg <TFTP/FTP server> <filename>
Saving the Active Switch Configuration

When the ptcfg command is used, the switch's active configuration commands (as displayed using /cfg/dump) will be uploaded to the specified script configuration file on the FTP/TFTP server. To start the switch configuration upload, at the Configuration# prompt, enter:

```
Configuration# ptcfg <FTP/TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IP address or hostname, and *filename* is the name of the target script configuration file.

NOTE – The output file is formatted with line-breaks but no carriage returns—the file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

NOTE – If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified ptcfg file must exist prior to executing the ptcfg command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

/cfg/gtcfg <FTP/TFTP server> <filename>
Restoring the Active Switch Configuration

When the gtcfg command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration. The configuration loaded using gtcfg is not activated until the apply command is used. If the apply command is found in the configuration script file loaded using this command, the apply action will be performed automatically.

To start the switch configuration download, at the Configuration# prompt, enter:

```
Configuration# gtcfg <FTP/TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IP address or hostname, and *filename* is the name of the target script configuration file.

CHAPTER 7

The Operations Menu

The Operations Menu is generally used for commands that affect switch performance immediately, but do not alter permanent switch configurations. For example, you can use the Operations Menu to immediately disable a port (without the need to apply or save the change), with the understanding that when the switch is reset, the port returns to its normally configured operation.

/oper
Operations Menu

```
[Operations Menu]
     port     - Operational Port Menu
     sys      - Operational System Menu
     passwd   - Change current user password
     clrlog   - Clear syslog messages
     tnetsshc - Close all telnet/SSH connections
     ntpreq   - Send NTP request
```

The commands of the Operations Menu enable you to alter switch operational characteristics without affecting switch configuration.

Table 7-1 Operations Menu (/oper)

Command Syntax and Usage
port *<port number>* Displays the Operational Port Menu. To view menu options, see page 202.
sys Displays the Operational System Menu. To view menu options, see page 203.
passwd *<1-128 characters>* Allows the user to change the password. You need to enter the current password in use for validation.

Table 7-1 Operations Menu (/oper)

Command Syntax and Usage
clrlog Clears all Syslog messages.
tnetsshc Closes all open Telnet and SSH connections.
ntpreq Allows the user to send requests to the NTP server.

/oper/port <port number>
Operations-Level Port Options

```
[Operations Port 1:1 Menu]
     8021x     - 8021.x Menu
     ena       - Enable port
     dis       - Disable port
     cur       - Current port state
```

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

Table 7-2 Operations-Level Port Menu Options (/oper/port)

Command Syntax and Usage
8021x Displays the 802.1X Port Menu. To view menu options, see page 203.
ena Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.
dis Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.
cur Displays the current settings for the port.

/oper/port <port number>/8021x
Operations-Level Port 802.1X Options

```
[802.1X Operation Menu]
     reset    - Reinitialize 802.1X access control on this port
     reauth   - Initiate reauthentication on this port now
```

Operations-level port 802.1X options are used to temporarily set 802.1X parameters for a port.

Table 7-3 Operations-Level Port 802.1X Menu Options (/oper/port x/8021x)

Command Syntax and Usage
reset Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration: ■ **force unauth** - the port is placed in unauthorized state, and traffic is blocked. ■ **auto** - the port is placed in unauthorized state, then authentication is initiated. ■ **force auth** - the port is placed in authorized state, and authentication is not required.
reauth Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as `auto`.

/oper/sys
Operational System Options

```
[Operational System Menu]
     i2c      - System I2C
```

Table 7-4 Operational System menu options (/oper/sys)

Command Syntax and Usage
i2c Displays the operational system-level I2C menu. I2C commands are used by Technical Support personnel.

CHAPTER 8

The Boot Options Menu

To use the Boot Options Menu, you must be logged in to the switch as the administrator. The Boot Options Menu provides options for:

- Selecting a switch software image to be used when the switch is next reset
- Selecting a configuration block to be used when the switch is next reset
- Downloading or uploading a new software image to the switch via FTP/TFTP

In addition to the Boot Menu, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to "Working with Switch Images and Configuration Files" on page 374.

/boot
Boot Menu

```
[Boot Options Menu]
     stack    - Stacking Menu
     image    - Select software image to use on next boot
     conf     - Select config block to use on next boot
     mode     - Select CLI mode to use on next boot
     prompt   - Prompt for selectable CLI mode
     gtimg    - Download new software image via FTP/TFTP
     ptimg    - Upload selected software image via FTP/TFTP
     reset    - Reset switch
     cur      - Display current boot options
```

Each of these options is discussed in greater detail in the following sections.

Stacking Boot Options

The Stacking Boot menu is used to define the role of the switch in a stack: either as the Master that controls the stack, or as a participating Member switch. Options are available for loading stack software to individual Member switches, and to configure the VLAN that is reserved for inter-switch stacking communications.

/boot/stack
Stacking Boot Menu

```
[Boot Stacking Menu]
     mode     - Set the stacking mode for the switch
     vlan     - Set VLAN number for control communication
     clear    - Set stacking parameters to factory default
     pushimg  - Push image to a switch in the stack
     cur      - Display current stacking boot parameters
```

Table 8-1 Stacking Boot menu (/boot/stack)

Command Syntax and Usage
mode master|member Configures the Stacking mode for the selected switch.
vlan *<VLAN number>* Configures the VLAN used for Stacking control communication.
clear Resets the Stacking boot parameters to their default values.
pushimg image1|image2|boot Pushes the selected software file from the master to the selected switch.
cur Displays current Stacking boot parameters.

Updating the Switch Software Image

The switch software image is the executable code running on the switch. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software available for your G8000, go to:

http://www.bladenetwork.net/support_services_rackswitch.html

Click on **`software updates`**. Use the `/boot/cur` command to determine the current software version.

The typical upgrade process for the software image consists of the following steps:

- Load the new boot image and software image onto a TFTP server on your network.
- Transfer the new boot image and software image from the TFTP server to your switch.
- Select the new software image to be loaded into switch memory the next time the switch is reset.

Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

Using the BLADE OS CLI

To load a new software image to your switch, you need the following:

- The image or boot software loaded on a TFTP server on your network
- The hostname or IP address of the TFTP server
- The name of the new software image or boot file

NOTE – The DNS parameters must be configured if specifying hostnames. See "Domain Name System Configuration" on page 184.

When the above requirements are met, use the following procedure to download the new software to your switch.

1. **At the `Boot Options#` prompt, enter:**

```
Boot Options# gtimg
```

2. **Enter the name of the switch software to be replaced:**

```
Enter name of switch software image to be replaced
 ["image1"/"image2"/"boot"]: <image>
```

3. **Enter the hostname or IP address of the TFTP server.**

```
Enter hostname or IP address of TFTP server: <name or IP address>
```

4. **Enter the name of the new software file on the server.**

```
Enter name of file on TFTP server: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the TFTP directory (usually `/tftpboot`).

5. **The system prompts you to confirm your request.**

You should next select a software image to run, as described below.

Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. **At the `Boot Options#` prompt, enter:**

```
Boot Options# image
```

2. **Enter the name of the image you want the switch to use upon the next boot.**

The system informs you of which image is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use switch software "image1" on next reset.
Specify new image to use on next reset ["image1"/"image2"]:
```

Uploading a Software Image from Your Switch

You can upload a software image from the switch to a TFTP server.

1. **At the `Boot Options#` prompt, enter:**

```
Boot Options# ptimg
```

2. **The system prompts you for information. Enter the desired image:**

```
Enter name of switch software image to be uploaded
["image1"|"image2"|"boot"]: <image>
```

3. **Enter the name or the IP address of the TFTP server:**

```
Enter hostname or IP address of TFTP server: <name or IP address>
```

4. **Enter the name of the file into which the image will be uploaded on the TFTP server:**

```
Enter name of file on TFTP server: <filename>
```

5. **The system then requests confirmation of what you have entered. To have the file uploaded, enter Y.**

```
image2 currently contains Software Version 1.0.1
 that was downloaded at  0:23:39 Thu Jan  4, 2009.
Upload will transfer image2 (2788535 bytes) to file "image1"
 on TFTP server 1.90.90.95.
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the G8000, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform the `save` command, your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your G8000 was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured G8000 is moved to a network environment where it will be re configured for a different purpose.

Use the following procedure to set which configuration block you want the switch to load the next time it is reset:

1. **At the `Boot Options#` prompt, enter:**

```
Boot Options# conf
```

2. **Enter the name of the configuration block you want the switch to use:**

   The system informs you of which configuration block is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use active configuration block on next reset.
Specify new block to use ["active"/"backup"/"factory"]:
```

Resetting the Switch

You can reset the switch to make your software image file and configuration block changes occur.

To reset the switch, at the `Boot Options#` prompt, enter:

```
>> Boot Options# reset
```

You are prompted to confirm your request.

Accessing the ISCLI

The default command-line interface for the switch is the BLADE OS CLI. To access the ISCLI, enter the following command and reset the switch:

```
Main# boot/mode iscli
```

To access the BLADE OS CLI, enter the following command from the ISCLI and reload the switch:

```
Router(config)# boot cli-mode blade-os
```

Users can select the CLI mode upon login, if the `/boot/prompt` command is enabled. Only an administrator connected through the CLI can view and enable `/boot/prompt`. When `/boot/prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

Using the Boot Management menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press the **<Shift>** key and the **<B>** key at the same time. The Boot Management menu appears.

```
Resetting the System ...
Memory Test ..............................

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Xmodem download
4 - Exit

Please choose your menu option: 1
Current boot image is 1. Enter image to boot: 1 or 2: 2
Booting from image 2
```

The Boot Management menu allows you to perform the following actions:

- To change the boot image, press 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To perform an Xmodem download, press 3 and follow the screen prompts.
- To exit the Boot Management menu, press 4. The boot process continues.

Using SNMP with Switch Images and Configuration Files

This section describes how to use MIB calls to work with switch images and configuration files. You can use a standard SNMP tool to perform the actions, using the MIBs listed in Table 8-2.

The examples in this section use the MIB name, but you can also use the OID.

Table 8-2 lists the MIBS used to perform operations associated with the G8000 switch image and configuration files. These MIBS are contained within in the file "g8000.mib"

Table 8-2 MIBs for Switch Image and Configuration Files

MIB Name	MIB OID
agTftpServer	1.3.6.1.4.1.26543.100.100.17.3.1.0
agTftpImage	1.3.6.1.4.1.26543.100.100.17.3.2.0
agTftpImageFileName	1.3.6.1.4.1.26543.100.100.17.3.3.0
agTftpCfgFileName	1.3.6.1.4.1.26543.100.100.17.3.4.0
agTftpAction	1.3.6.1.4.1.26543.100.100.17.3.5.0
agTftpLastActionStatus	1.3.6.1.4.1.26543.100.100.17.3.6.0

The following SNMP actions can be performed using the MIBs listed in Table 8-2.

- Load a new Switch image (boot or running) from a TFTP server.
- Load a previously saved switch configuration from a TFTP server.
- Save the switch configuration to a TFTP server.

Loading a new switch image

To load a new switch image with the name "MyNewImage.img" into `image2`, follow the steps below. This example assumes you have a TFTP server at 192.168.10.10.

1. **Set the TFTP server address where the switch image resides:**

   ```
   Set agTftpServer.0 "192.168.10.10"
   ```

2. **Set the area where the new image will be loaded:**

   ```
   Set agTftpImage.0 "image2"
   ```

3. **Set the name of the image:**

   ```
   Set agTftpImageFileName.0 "MyNewImage.img"
   ```

4. **Initiate the transfer. To transfer a switch image, enter 2 (get image):**

   ```
   Set agTftpAction.0 "2"
   ```

5. **Verify the transfer:**

   ```
   Get agTftpLastActionStatus.0
   ```

Loading a switch configuration to the active configuration

Use this procedure to load a saved switch configuration ("MyActiveConfig.cfg") into the active configuration block. This example assumes you have a TFTP server at 192.168.10.10.

1. **Set the TFTP server address where the switch Configuration File resides:**

   ```
   Set agTftpServer.0 "192.168.10.10"
   ```

2. **Set the name of the configuration file:**

   ```
   Set agTftpCfgFileName.0 "MyActiveConfig.cfg"
   ```

3. **Initiate the transfer. To restore a running configuration, enter 12 (get config):**

   ```
   Set agTftpAction.0 "12"
   ```

4. **Verify the transfer:**

   ```
   Get agTftpLastActionStatus.0
   ```

Saving the switch configuration from the active configuration

To save the active switch configuration to a TFTP server follow the steps below. This example assumes you have a TFTP server at 192.168.10.10.

1. **Set the TFTP server address where the configuration file is saved:**

   ```
   Set agTftpServer.0 "192.168.10.10"
   ```

2. **Set the name of the configuration file:**

   ```
   Set agTftpCfgFileName.0 "MyActiveConfig.cfg"
   ```

3. **Initiate the transfer. To save a running configuration file, enter 13 (put config):**

   ```
   Set agTftpAction.0 "13"
   ```

4. **Verify the transfer:**

   ```
   Get agTftpLastActionStatus.0
   ```

CHAPTER 9

The Maintenance Menu

The Maintenance Menu is used to manage dump information and forward database information. It also includes a debugging menu to help with troubleshooting.

/maint
Maintenance Menu

NOTE – To use the Maintenance Menu, you must be logged in to the switch as the administrator.

```
[Maintenance Menu]
     sys       - System Maintenance Menu
     fdb       - Forwarding Database Manipulation Menu
     debug     - Debugging Menu
     arp       - ARP Cache Manipulation Menu
     igmp      - IGMP Multicast Group Menu
     uudmp     - Uuencode FLASH dump
     ptdmp     - Upload FLASH dump via FTP/TFTP
     ptlog     - Upload file via TFTP
     cldmp     - Clear FLASH dump
     tsdmp     - Tech support dump
     pttsdmp   - Upload tech support dump via FTP/TFTP
```

Dump information contains internal switch state data that is written to flash memory on the G8000 after any one of the following occurs:

- The switch administrator forces a switch *panic*. The `panic` option, found in the Maintenance Menu, causes the switch to dump state information to flash memory, and then causes the switch to reboot.
- The watchdog timer forces a switch reset. The purpose of the watchdog timer is to reboot the switch if the switch software freezes.
- The switch detects a hardware or software problem that requires a reboot.

Table 9-1 Maintenance Menu (/maint)

Command Syntax and Usage
sys Displays the System Maintenance Menu. To view menu options, see page 219.
fdb Displays the Forwarding Database Manipulation Menu. To view menu options, see page 220.
debug Displays the Debugging Menu. To view menu options, see page 221.
arp Displays the ARP Cache Manipulation Menu. To view menu options, see page 222.
igmp Displays the IGMP Maintenance Menu. To view menu options, see page 223.
uudmp Displays dump information in uuencoded format. For details, see page 225.
ptdmp hostname filename Saves the system dump information via FTP/TFTP. For details, see page 225.
ptlog Uploads a specified syslog file from the switch to a FTP/TFTP server.
cldmp Clears dump information from flash memory. For details, see page 226.
tsdmp Dumps all G8000 information, statistics, and configuration.You can log the tsdump output into a file.
pttsdmp Redirects the technical support dump (tsdmp) to an external TFTP server.

/maint/sys
System Maintenance

This menu is reserved for use by Technical Support personnel. The options are used to perform system debugging.

```
[System Maintenance Menu]
      flags   - Set NVRAM flag word
      tmask   - Set MP trace mask word
```

Table 9-2 System Maintenance Menu Options (/maint/sys)

Command Syntax and Usage
flags *<new NVRAM flags word as 0xXXXXXXXX>* This command sets the flags that are used for debugging purposes by Technical Support personnel.
tmask *<new trace mask word as 0xXXXXXXXX>* **[p]** This command sets the trace mask that is used for debugging purposes by Technical Support personnel.

/maint/fdb
Forwarding Database Maintenance

```
[FDB Manipulation Menu]
      find    - Show a single FDB entry by MAC address
      port    - Show FDB entries for a single port
      vlan    - Show FDB entries for a single VLAN
      dump    - Show all FDB entries
      del     - Delete an FDB entry
      clear   - Clear entire FDB
```

The Forwarding Database Manipulation Menu can be used to view information and to delete a MAC address from the forwarding database or clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

Table 9-3 FDB Manipulation Menu Options (/maint/fdb)

Command Syntax and Usage
find *<MAC address>* [*<VLAN>*] Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the `xx:xx:xx:xx:xx:xx` format (such as `08:00:20:12:34:56`) or `xxxxxxxxxxxx` format (such as `080020123456`).
port *<port number>* Displays all FDB entries for a particular port.
vlan *<VLAN number (1-4095)>* Displays all FDB entries on a single VLAN.
dump Displays all entries in the Forwarding Database. For details, see page 52.
del *<MAC address>* [*<VLAN>*] Removes a single FDB entry.
clear Clears the entire Forwarding Database from switch memory.

/maint/debug
Debugging Options

```
[Miscellaneous Debug Menu]
     tbuf     - Show MP trace buffer
     snap     - Show MP snap (or post-mortem) trace buffer
     clrcfg   - Clear all flash configs
```

The Miscellaneous Debug Menu displays trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug menu:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reset occurs

If the switch resets for any reason, the MP trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by Technical Support personnel.

Table 9-4 Miscellaneous Debug Menu Options (/maint/debug)

Command Syntax and Usage
tbuf Displays the Management Processor trace buffer. Header information similar to the following is shown: `MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748` The buffer information is displayed after the header.
snap Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred.
clrcfg Deletes all flash configuration blocks.

/maint/arp
ARP Cache Maintenance

```
[Address Resolution Protocol Menu]
     find     - Show a single ARP entry by IP address
     port     - Show ARP entries on a single port
     vlan     - Show ARP entries on a single VLAN
     addr     - Show ARP entries for switch's interfaces
     dump     - Show all ARP entries
     clear    - Clear ARP cache
```

Table 9-5 ARP Maintenance Menu Options (/maint/arp)

Command Syntax and Usage
find *<IP address (such as, 192.4.17.101)>* Shows a single ARP entry by IP address.
port *<port number>* Shows ARP entries on a single port.
vlan *<VLAN number>* Shows ARP entries on a single VLAN.
addr Shows the list of IP addresses which the switch will respond to for ARP requests.
dump Shows all ARP entries.
clear Clears the entire ARP list from switch memory.

NOTE – To display all ARP entries currently held in the switch, or a portion according to one of the options listed on the menu above (`find`, `port`, `vlan`, `dump`), you can also refer to "ARP Information" on page 61.

/maint/igmp
IGMP Maintenance

```
[IGMP Multicast Group Menu]
     group    - Multicast Group Menu
     mrouter  - IGMP Multicast Router Port Menu
     clear    - Clear group and mrouter tables
```

Table 9-6 describes the IGMP Maintenance commands.

Table 9-6 IGMP Maintenance Menu Options (/maint/igmp)

Command Syntax and Usage
group Displays the Multicast Group menu. To view menu options, see page 223.
mrouter Displays the Multicast Router Port menu. To view menu options, see page 224.
clear Clears the IGMP group table and Mrouter tables.

/maint/igmp/group
IGMP Group Maintenance

```
[IGMP Multicast Group Menu]
     find     - Show a single group by IP group address
     vlan     - Show groups on a single vlan
     port     - Show groups on a single port
     trunk    - Show groups on a single trunk
     detail   - Show detail of a single group by IP address
     dump     - Show all groups
     clear    - Clear group tables
```

The following table describes the IGMP Maintenance commands.

Table 9-7 IGMP Multicast Group Maintenance Menu Options (/maint/igmp/group)

Command Syntax and Usage
find *<IP address>* Displays a single IGMP multicast group by its IP address.
vlan *<VLAN number>* Displays all IGMP multicast groups on a single VLAN.

Table 9-7 IGMP Multicast Group Maintenance Menu Options (/maint/igmp/group)

Command Syntax and Usage
port *<port number>* Displays all IGMP multicast groups on a single port.
trunk *<trunk number>* Displays all IGMP multicast groups on a single trunk group.
detail *<IP address>* Displays detailed information about a single IGMP multicast group.
dump Displays information for all multicast groups.
clear Clears the IGMP group tables.

/maint/igmp/mrouter

IGMP Multicast Routers Maintenance

```
[IGMP Multicast Routers Menu]
     vlan     - Show all multicast router ports on a single vlan
     dump     - Show all multicast router ports
     clear    - Clear multicast router port table
```

The following table describes the IGMP multicast router (Mrouter) maintenance commands.

Table 9-8 IGMP Mrouter Maintenance Menu Options (/maint/igmp/mrouter)

Command Syntax and Usage
vlan *<VLAN number>* Shows all IGMP multicast router ports on a single VLAN.
dump Shows all multicast router ports.
clear Clears the IGMP Multicast Router port table.

/maint/uudmp
Uuencode Flash Dump

Using this command, dump information is presented in uuencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `uudmp` command. This will ensure that you do not lose any information. Once entered, the `uudmp` command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the `uudmp` command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

NOTE – Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see page 226.

To access dump information, at the `Maintenance#` prompt, enter:

```
Maintenance# uudmp
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following appears:

```
No FLASH dump available.
```

/maint/ptdmp *<FTP/TFTP server> <filename>*
FTP/TFTP System Dump Put

Use this command to `put` (save) the system dump to a FTP/TFTP server.

NOTE – If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified `ptdmp` file must exist *prior* to executing the `ptdmp` command, and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via FTP/TFTP, at the `Maintenance#` prompt, enter:

```
Maintenance# ptdmp <FTP/TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IP address or hostname, and *filename* is the target dump file.

/maint/cldmp

Clearing Dump Information

To clear dump information from flash memory, at the `Maintenance#` prompt, enter:

```
Maintenance# cldmp
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

Unscheduled System Dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Tuesday March 14, 2009. Use /maint/uudmp to
      extract the dump for analysis and /maint/cldmp to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```

Index

Symbols

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W